5-24-2016

Exploration of Physical Layer Security in Underwater Acoustic Communications

Yi Huang
University of Connecticut - Storrs, yi.huang@uconn.edu

Exploration of Physical Layer Security in Underwater Acoustic Communications

Yi Huang, Ph.D.

University of Connecticut, 2016

Physical layer security has been under extensive investigation in recent years in wireless radio communications. However, its study in the context of underwater acoustic (UWA) communications is very limited. This dissertation will explore the fundamental properties of UWA channels to achieve physical layer security. It includes three research topics: 1) Channel estimation in UWA systems leveraging the inherent channel sparsity; 2) Secret key generation through the reciprocity of UWA channels; 3) Self-protection jamming in half-duplex systems leveraging large propagation delays.

The first part of the dissertation deals with sparse channel estimation in UWA orthogonal frequency division multiplexing (OFDM) systems. By exploiting the sparse nature of UWA channels, compressed sensing (CS) based channel estimation methods have demonstrated superior performance compared to conventional least-squares (LS) methods. However, *a priori* information of channel sparsity level is required to set the regularization parameter properly. We propose a data-driven sparsity learning approach based on a linear minimum mean squared error (LMMSE) equalizer to tune the regularization parameter for OFDM transmissions.

The second part of the dissertation focuses on secret key generation in UWA channels. Predefined secret keys are often used to encrypt information. However, they could be leaked to eavesdroppers. A key generation protocol is presented where secret keys are dynamically generated by quantizing the measured amplitudes on OFDM subcarriers, and then using error correction codes for secret bits extraction according to the Slepian-Wolf coding principle. By analyzing the performance based on collected field data, an improved key generation protocol is proposed by incorporating two modules to increase the channel correlation and deal with channel dynamics.

The last part of the dissertation presents a self-protection jamming approach for block transmissions in half-duplex UWA systems. Different from existing approaches, where additional helpers (e.g., relays) are needed to transmit jamming signals, the proposed protocol does not need any helper but instead relies on the legitimate receiver itself. This approach exploits the half-duplex nature of underwater transceivers and the block-based transmission structure, by taking advantage of the large propagation delays to create interference at the eavesdropper without affecting the reception of the intended user.

Exploration of Physical Layer Security in Underwater Acoustic Communications

Yi Huang

B.S., Northwestern Polytechnical University, Xi'an, China, 2008
M.S., Northwestern Polytechnical University, Xi'an, China, 2011

A Dissertation

Submitted in Partial Fulfillment of the

Requirements for the Degree of Doctor of Philosophy

at the

University of Connecticut

2016

APPROVAL PAGE

Doctor of Philosophy Dissertation

Exploration of Physical Layer Security in Underwater Acoustic Communications

Presented by

Yi Huang, B.S., M.S.

Major Advisor _____
Rajeev Bansal

Associate Advisor _____
Peter Willett

Associate Advisor _____
Shalabh Gupta

University of Connecticut

2016

To my family

ACKNOWLEDGEMENTS

First, I want to express my heartfelt gratitude to Professor Shengli Zhou for his excellent guidance, constant support, and providing me the precious opportunity to pursue my Ph.D. in UCONN. I can ever express what the experience means to me and how much it shapes me. He encouraged me to collaborate with others in teamwork, and trained me to be a coordinator and mentor in projects whenever possible. His sharp insight, broad knowledge, creative and critical thinking, and down-to-earth attitude set me an outstanding example of academic perfection. I attribute this dissertation to his effort and assistance.

I am also extremely grateful to my major advisor Professor Rajeev Bansal for his help and advice. The acknowledgement also goes to Professor Zhijie Shi for his supervision in my research. They are so nice and professional, and sets a good example to me, which will continue to benefit the rest of my life.

I would like to thank Professor Peter Willett, Professor Shalabh Gupta, Professor Yaakov Bar-Shalom, Professor Song Han, Professor Bing Wang, Professor Pattipati, Professor Marten and Dr. Athanasios Bamis for their broad knowledge and heuristic advice. It is fabulously intriguing to get inspired by their cool achievements and exceptional creativity.

I want to thank my colleagues and lab mates Lei Wan, Zhaohui Wang, Jianzhong Huang, Xiufeng Song, Hao Zhou, Xiaoka Xu, Huizhong Gao, Qin Lu, Sharief Abdel-Razeq, Patrick Carroll, Katherine Domrese, Yuzhi Zhang, Yougan Chen, Xiaoyan Kuai, Lu Ma, Wei Li, Xingyu Cai, Peng Xiao, and my lab mates/neighbors Mingyang Li, Wenbo Dou, Djedjiga Belfadel, Ting Yuan for their helpful discussions in my research, and advice on my career.

I also would like to thank my friends in UCONN, Junlin Chen, Guoxian Huang, Dongqiao Zhang and Dong Zhao, etc, for their thoughtful support and companion in my hard time. The happiness and woe we shared make the life here an amazing and unforgettable journey.

Last and foremost, I give my deepest and sincerest gratitude to my parents, Youkang Huang, and Qunying Zhang, for their endless love, understanding, encouragement, and belief in my life. Their unconditional generosity and support have been my inspiration to accomplish my doctoral program, and raise me to more than I can be. To my family, I dedicate this dissertation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Acronyms and Notations

Acronym

ACK	acknowledgement
AF	amplify-and-forward
ARMA	autoregressive-moving-average
BCH	Bose, Chaudhuri, and Hocquenghem
BER	bit error rate
BIC	Bayesian information criterion
BitMR	bit match rate
BJ	barrage jamming
BLER	block error rate
BP	basis pursuit
BurstMR	burst match rate
CDF	cumulative distribution function
CFO	carrier frequency offset
CFR	channel frequency response

CGC	channel gain complement
CIR	channel impulse response
CJ	cooperative jamming
CP	cyclic prefix
CS	compressed sensing
DCT	discrete cosine transformation
DF	decode-and-forward
FD	full-duplex
FFT	fast Fourier transform
GCV	generalized cross validation
GML	generalized maximum likelihood
ICI	inter-carrier interference
i.i.d.	identically and independently distributed
IST	iterative shrinkage/threshold
IRS	iterative reweighted shrinkage
LDPC	low-density parity-check
LMMSE	linear minimum mean squared error
LS	least-squares
MAP	maximum a-posteriori probability
MDL	minimal description length
MIMO	multiple-input multiple-output

MNDL	minimum noiseless description length
MP	matching pursuit
MSE	mean squared error
OFDM	orthogonal frequency division multiplexing
PMI	precoding matrix index
QPSK	quadrature phase-shift keying
RMSE	root mean squared error
RSS	received signal strength
RSSI	received signal strength indicators
SIMO	single-input multi-output
SINR	signal-to-interference-and-noise ratio
SISO	single-input single-output
SNR	signal-to-noise ratio
SPACE08	2008 Surface Processes and Acoustic Communications Experiment
SURE	Stein's unbiased risk estimation
TL	transmission loss
UWA	underwater acoustic
WSN	wireless sensor network
ZP	zero-padded

Notation

x	scalar
$\mathbf{x}$	vector
$\mathbf{X}$	matrix
$\propto$	equality of functions up to a scaling factor
$\mathbf{x}[m]$	the mth entry of vector $\mathbf{x}$
$\mathbf{X}[m, n]$	the (m, n)th entry of matrix $\mathbf{X}$
$(\cdot)^*$	conjugate
$(\cdot)^T$	matrix transpose
$(\cdot)^H$	Hermitian transpose
$\mathbf{I}_k$	$k \times k$ identity matrix
$\lvert \cdot \rvert$	absolute
$\lVert \cdot \rVert_n$	n-th norm

Chapter 1

Introduction

1.1 Motivation

Physical layer security is an important research topic. The research on physical layer security in radio communications has been ongoing for decades. However, the research on physical layer security in UWA communications is at an early stage.

Shannon introduced the concept of perfect secrecy in [99], where a shared secret key at least as long as the message was required to achieve information-theoretically secure communication by one-time pad encryption, resulting the random guess as the best strategy for the eavesdropper to retrieve the transmitted message. Wyner suggested the weak secrecy of a system if the leaked information rate is asymptotically zero in the codeword length [121]. The pioneer work of Wyner reveals that if the eavesdropper's channel is a degraded version of the channel between the source and the destination, the information-theoretically secure communication between legitimate

users at a non-zero rate is feasible without using any secret keys. Csiszár and Körner generalized Wyner's results to the cases of non-degraded channels, where information-theoretically secure communication is realizable by taking advantage of the inherent channel randomness [32].

In radio communications, the approaches to guarantee secrecy against eavesdropping at the physical layer can be divided into two categories [14]. One is on secret key generation, which is the source model based physical layer security approach. The characteristics of wireless channels can be used to extract secret keys for encryption, based on the reciprocity and randomness of the channels [78]. The time, frequency, space, and multipath diversity of channels can be used for key extraction. The other one is on information-theoretic security based on jamming, which is characterized as the channel model based physical layer security approach. Cooperative jamming and interference alignment are two popular methods to improve the secrecy rate [81], where "Barrage Jamming" (BJ) or full noise jamming is usually exploited for theoretical analysis. Barrage jamming can interfere the eavesdropper by transmitting artificial noise within the signal bandwidth [7]. If the transmitted waveform is known, the jammer can design a better jamming strategy than BJ, and achieve higher bit error rate (BER) with less jamming power. Ref. [98] showed that jamming the pilot subcarriers of OFDM symbols could lead to higher BER than barrage jamming. If the pilot information is shared between legitimate users, superimposed pilot jamming can secure the communication between the legitimate users without any helpers, where the superimposed pilots act as the artificial noise [27].

Due to the fast speed of the electromagnetic wave (3×10^8 m/s), all the research on physical layer security in radio communications neglects the propagation delay and assumes that the received signals are perfectly synchronized. The key generation process and jamming protocols are assumed to be within the channel coherence time. As such, the helpers can optimize their transmission to achieve interference cancellation or interference alignment by exploiting the spatial orthogonality in both half-duplex and full-duplex systems, and secret keys can be extracted from the stable channels within the coherence time. However, underwater acoustic channels are time-varying and differ from radio channels drastically. The UWA channel suffers from long propagation delay and severe Doppler effects, due to the low acoustic speed in water (around 1500 m/s) [76, 104]. The assumptions in radio communications no longer hold in UWA communications. The research in this dissertation provides a timely investigation of physical layer security in the context of UWA communications.

1.2 Outline of the Dissertation

Chapter 2 introduces the sparse channel estimation for underwater acoustic OFDM with data-driven sparsity learning, which helps to gain a deep understanding of the channel multipath structure.

Chapter 3 investigates secret key generation based on the frequency response of the estimated UWA channels, where the reciprocity of mutual channels will be validated by data collected from field experiments and the data by simulations.

Chapter 4 presents a half-duplex jamming approach for block transmissions over UWA channels, where the propagation delay plays an important role.

Chapter 5 concludes the dissertation.

1.3 Publications

The results from the following publications have been included in this thesis.

Journal papers:

- [J1] **Y. Huang**, S. Zhou, Z. Shi, and L. Lai, "Channel frequency response based secret key generation in underwater acoustic systems," *IEEE Transactions on Wireless Communications*, May 2016 (Accepted).

- [J2] **Y. Huang**, P. Xiao, S. Zhou and Z. Shi, "A half-duplex self-protection jamming approach for improving secrecy of block transmissions in underwater acoustic channels," *IEEE Sensors Journal*, vol. 16, no. 11, pp. 4100–4109, Jun. 2016.

- [J3] **Y. Huang**, L. Wan, S. Zhou, Z. Wang, and J. Huang, "Comparison of sparse recovery algorithms for channel estimation in underwater acoustic OFDM with data-driven sparsity learning," *Elsevier Journal on Physical Communication*, vol. 13, pp. 156–167, Dec. 2014.

Conference papers:

- [C1] **Y. Huang**, S. Zhou, Z. Shi, and L. Lai, "Experimental study of secret key generation in underwater acoustic channels," *in Proc. of the Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA., Nov. 2014.

The results from the following papers have not been included in this thesis.

Journal papers:

- [J4] L. Wan, H. Zhou, X. Xu, **Y. Huang**, S. Zhou, Z. Shi and J-H. Cui, "Adaptive modulation and coding for underwater acoustic OFDM," *IEEE Journal of Oceanic Engineering*, vol. 40, no. 2, pp. 327-336, Apr. 2015.

- [J5] Y. Zhang, **Y. Huang**, L. Wan, S. Zhou, X. Shen, and H. Wang, "Adaptive OFDMA with partial CSI feedback for underwater acoustic communications," *Journal of Communications and Networks*, Aug. 2015 (Accepted).

- [J6] X. Cai, L. Wan, **Y. Huang**, S. Zhou and Z. Shi, "Further results on multicarrier MFSK based underwater acoustic communications," *Elsevier Journal on Physical Communication*, vol. 18, pp. 15–27, Mar. 2016.

Conference papers:

- [C2] Y. Su, Y. Zhang, S. Le, H. Mo, L. Wei, **Y. Huang**, Z. Peng, and J. Cui, "A versatile lab testbed for underwater sensor networks," *in Proc. of IEEE/MTS OCEANS conference*, San Diego, CA, vol. 1, no. 5, pp. 23–27, Sep. 2013.

- [C3] L. Wan, H. Zhou, X. Xu, **Y. Huang**, S. Zhou, Z. Shi and J.-H. Cui, "Field test of adaptive modulation and coding for underwater acoustic OFDM," *in*

Proc. of the ACM International Workshop on UnderWater Networks (WUWNet), Kaohsiung, Taiwan, Nov. 2013.

- [C4] Y. Zhang, **Y. Huang**, L. Wan, H. Zhou, S. Zhou, X. Shen, and H. Wang, "Adaptive OFDMA for downlink underwater acoustic communications," *in Proc. of IEEE/MTS OCEANS conference*, St. John's, Canada, vol. 1, no. 5, pp. 14–19, Sep. 2014.

- [C5] Q. Lu, **Y. Huang**, Z. Wang, and S. Zhou, "Characterization and receiver design for underwater acoustic channels with large doppler spread," *in Proc. of IEEE/MTS OCEANS conference*, Washington, D. C., Oct. 2015.

Chapter 2

Comparison of Sparse Recovery Algorithms for Channel Estimation in Underwater Acoustic OFDM with Data-Driven Sparsity Learning

2.1 Introduction

Underwater acoustic (UWA) channels are often characterized as doubly (time- and frequency-) selective channels due to the large delay and Doppler spreads [37, 88, 89, 111, 136]. The UWA communication performance largely hinges on the channel estimation accuracy at the receiver. Recent research progress on UWA channel estimation [11, 16, 44, 61, 64, 66] has demonstrated that sparse channel estimation, which exploits the inherent sparsity in UWA channels, leads to better receiver decoding performance than the conventional least-squares (LS) based channel estimation.

For block transmissions in UWA environments, different channel models have been explored for channel estimation, see e.g., [11, 16, 61, 92, 123]. Consider a block transmission with the channel outputs collected in a vector $\mathbf{z}$ and the channel unknown parameters collected in a vector $\mathbf{x}$. A sparse channel estimation can be formulated as an L_q-norm based optimization problem:

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \frac{1}{2}\|\mathbf{z} - \mathbf{A}\mathbf{x}\|_2^2 + \lambda\|\mathbf{x}\|_q^q, \quad 0 \leq q \leq 2 \tag{1}$$

where the first item is the fitting error with $\mathbf{A}$ being a suitable mixing matrix, the second term promotes the sparsity of the solution $\hat{\mathbf{x}}$, $\|\cdot\|_q$ denotes the L_q norm of a vector, and λ is the regularization parameter which trades off the fitting error and the sparsity of the solution.

Different values of parameter q in (1) dictate different optimization problems. The regularized L_2 problem could be called a sparse least-squares problem but the solution may be not sparse with high probability [83]. A series of greedy algorithms based on matching pursuit (MP) aim to solve an NP-hard L_0 problem. Many iterative shrinkage/threshold (IST) algorithms for L_1 problems, often referred as Basis pursuit (BP) or BP De-Nosing, thrive to solve a convex optimization L_1 problem in recent years, such as FISTA, TwIST, Nesterov, Homotopy, and ADM [9, 13, 82, 90]. Ref. [48] compared three BP algorithms: SpaRSA, l1_ls [58], and YALL1 algorithms in underwater environments, while [90] compared Homotopy and YALL1. To achieve a sparser solution without degrading the performance, a half thresholding algorithm is proposed in [124] to tackle an $L_{1/2}$ optimization problem, and is proven efficient in synthetic

aperture radar imaging processing [130]. In this chapter, we compare the performance of different L_q solvers for the UWA channel estimation.

In practice, the regularization parameter λ is unknown, and an inappropriate λ will considerably degrade the recovery performance. A lot of research has been carried out on how to select λ. For the L_2 problem, a modified L-curve method is proposed to overcome the non-robustness of the L-curve method, by utilizing prior information to define the bounds on λ [96]. For the L_0 problem, the information criteria that are first introduced in autoregressive−moving−average (ARMA) model order selection is used to select λ, e.g., the generalized maximum likelihood (GML) adopted in [91] and the Bayesian information criterion (BIC) in [66]. For the L_1 problem, ref. [5] adopts the BIC criterion to choose λ, ref. [84] proposes to use the minimal description length (MDL) to select λ based on a maximum a-posteriori probability (MAP) estimator aiming to find the minimal data error, while the minimum noiseless description length (MNDL) criterion extends the selection of λ to minimize the reconstruction error [87]. The mean square error (MSE), Stein's unbiased risk estimation (SURE) and generalized cross validation (GCV) methods are tested in both L_1 and L_2 problems, where the predictive risk and the signal estimation errors are minimized to select λ [8, 95]. As shown in [12], minimizing root mean square error (RMSE) with the original signal may not always be a good method. In this chapter, we propose a new approach that is called data-driven sparsity learning based on an LMMSE equalizer to tune the regularization parameter.

This chapter focuses on sparse channel estimation in an Orthogonal frequency division multiplexing (OFDM) system, which has been under extensive investigation in recent years [11,17,28,41,44,46,65,80,101,102,106,116,125,137]. The contributions of this chapter are summarized as follows.

1) We compare the decoding performance of the aforementioned L_q sparse recovery algorithms in the intercarrier interference (ICI)-ignorant and ICI-aware OFDM receivers, respectively, for $q = 0, 1/2, 1, 2$. Both simulation and experimental results reveal that the ICI-aware receiver outperforms the ICI-ignorant receiver for any L_q algorithm, and $L_{1/2}$ achieves nearly the same performance as L_1 algorithms, which outperform L_0 and L_2 algorithms.

2) We propose a data-driven sparsity learning approach based on an LMMSE equalizer to select the regularization parameter λ in OFDM block transmissions. The tuned λ in the first block will be used in the following blocks, and the golden section search is utilized to accelerate the sparsity learning process. Simulation and experimental results validate the effectiveness of the proposed approach.

The rest of the chapter is organized as follows. Section 2.2 briefly describes the system model. Section 2.3 introduces sparse channel estimation and several compressed sensing algorithms. Section 2.4 presents the data-driven sparsity learning approach based on an LMMSE equalizer. The simulation results are provided in Section 2.5. The experimental results are presented in Section 2.6. Finally, we draw conclusions in Section 2.7.

Notation: Bold lower case letters and upper case letters denote column vectors and matrices, respectively. $(\cdot)^T$ and $(\cdot)^H$ denote transpose and Hermitian transpose, respectively. $x[m]$ denotes the mth element of vector **x**, and $H[m,k]$ denotes the (m,k)th element of matrix **H**. **I** denotes the unit matrix. $\|\mathbf{x}\|_\infty$ denotes the maximum absolute value of elements of vector **x**.

2.2 System Model

The zero-padded (ZP) OFDM signal format is considered [61]. Let T denote the symbol duration, $T_{\rm g}$ the guard interval. The total OFDM block duration is $T_{\rm bl} = T + T_{\rm g}$. Let B denote the bandwidth and K the total number of subcarriers. The subcarrier spacing is $\triangle f = 1/T = B/K$. The mth subcarrier is at frequency

$$f_m = f_{\rm c} + \frac{m}{T}, \quad m = -\frac{K}{2}, \ldots, \frac{K}{2} - 1 \tag{2}$$

where $f_{\rm c}$ is the center frequency. The K subcarriers are divided into three non-overlapping sets: data subcarriers $\mathcal{S}_{\rm D}$, pilot subcarriers $\mathcal{S}_{\rm P}$, and null subcarriers $\mathcal{S}_{\rm N}$, which satisfy $\mathcal{S}_{\rm D} \cup \mathcal{S}_{\rm P} \cup \mathcal{S}_{\rm N} = \{-K/2, \ldots, K/2-1\}$. The numbers of corresponding subcarriers are $K_{\rm D}$, $K_{\rm P}$, and $K_{\rm N}$, which satisfy $K_{\rm D} + K_{\rm P} + K_{\rm N} = K$. Let $s[m]$ denote the symbol to be transmitted on the mth subcarrier. The transmitted signal of one ZP-OFDM block in passband is given by

$$\tilde{x}(t) = 2\mathrm{Re}\left\{ \Big[\sum_{m \in \mathcal{S}_{\rm D} \cup \mathcal{S}_{\rm P}} s[m] e^{j2\pi \frac{m}{T} t} g(t) \Big] e^{j2\pi f_{\rm c} t} \right\}, \quad t \in [0, T_{\rm bl}] \tag{3}$$

where $g(t)$ is a rectangular pulse-shaping window, whose Fourier transform is given by

$$G(f) = \frac{\sin(\pi f T)}{\pi f T} e^{-j\pi f T}. \tag{4}$$

2.2.1 Channel Model

The path-based time-varying underwater channel is modeled as

$$h(\tau, t) = \sum_{p=1}^{N_{\text{pa}}} A_p \delta\left(\tau - [\tau_p - a_p t]\right) \tag{5}$$

where N_{pa} is the number of paths, A_p, τ_p and a_p are the amplitude, delay and Doppler scaling factor of the pth path within one block duration, respectively. The received signal in passband is expressed as

$$\tilde{y}(t) = \sum_{p=1}^{N_{\text{pa}}} A_p \tilde{x}\left((1 + a_p)t - \tau_p\right) + \tilde{n}(t) \tag{6}$$

where $\tilde{n}(t)$ is the additive noise.

2.2.2 Receiver Model

The receiver adopts the two-step Doppler compensation method [61]. The Doppler scale $\hat{a}$ and the carrier frequency offset (CFO) $\hat{\epsilon}$ are estimated as described in [61] and [109]. The signal after the Doppler compensation can be expressed as: $\tilde{z}(t) = \tilde{y}(t/(1+\hat{a}))e^{-j2\pi\hat{\epsilon}t}$. The frequency-domain measurement on the mth subcarrier is then

$$z[m] = \int_0^{T_{\text{bl}}} \tilde{z}(t) e^{-j2\pi f_m t} dt = \sum_{k=-K/2}^{K/2-1} H[m,k]s[k] + n[m] \tag{7}$$

where $H[m,k]$ is the ICI coefficient that specifies how the symbol on the kth subcarrier contributes to the measurement on the mth subcarrier, and $n[m]$ is the additive noise. Using the banded-ICI assumption in [50] [49]

$$H[m,k] \simeq 0, \text{ if } |m-k| > D, \tag{8}$$

the system model becomes

$$z[m] = \sum_{k=m-D}^{m+D} H[m,k]s[k] + \eta[m], \tag{9}$$

where D denotes the ICI depth, and

$$\eta[m] = \sum_{|m-k|>D} H[m,k]s[k] + n[m]. \tag{10}$$

Using the matrix-vector notation, we have the compact input-output relationship as

$$\mathbf{z} \triangleq \mathbf{H}^D\mathbf{s} + \boldsymbol{\eta} \tag{11}$$

where $\mathbf{z}$ contains the measurements from all subcarriers, $\mathbf{s}$ contains all transmitted symbols, and $\mathbf{H}^D$ is the banded channel matrix with nonzero entries on the $2D+1$ diagonals.

Based on different assumptions on D, two kinds of OFDM receivers are developed:

- **ICI-aware receiver** $(D > 0)$: It reduces the computational complexity compared to the full ICI-aware receiver, and models the ICI effect with ICI-depth D in time-varying channels.

- **ICI-ignorant receiver** $(D = 0)$: It is a special case of ICI-aware receiver, where $\mathbf{H}^D$ is a diagonal matrix.

After the channel matrix $\mathbf{H}^D$ is estimated, the LMMSE equalizer [108] is used for symbol detection, and the details are discussed in Section 2.4.1. With the soft outputs from LMMSE, the rate $1/2$ nonbinary LDPC decoder proposed in [22, 51] will yield the decoded information symbols.

2.3 Channel Estimation

The ICI coefficient $H[m,k]$ in (7) can be represented by the $N_{\rm pa}$ path parameters as

$$H[m,k] = \sum_{p=1}^{N_{\rm pa}} \xi_p e^{-j2\pi \frac{m}{T}\bar{\tau}_p} G\left(\frac{f_m + \hat{\epsilon}}{1+b_p} - f_k\right) \tag{12}$$

where the complex gain ξ_p, the scaled delay $\bar{\tau}_p$, and the residual Doppler rate b_p are

$$b_p := \frac{a_p - \hat{a}}{1+\hat{a}}, \quad \bar{\tau}_p := \frac{\tau_p}{1+b_p}, \quad \xi_p := \frac{A_p}{1+b_p} e^{-j2\pi \frac{m}{T}\bar{\tau}_p}. \tag{13}$$

Define a $K \times K$ diagonal matrix $\mathbf{\Lambda}$ with entries of $[\mathbf{\Lambda}(\bar{\tau}_p)]_{m,m} = e^{-j2\pi \frac{m}{T}\bar{\tau}_p}$, and another $K \times K$ matrix $\mathbf{\Gamma}$ with entries of $[\mathbf{\Gamma}(b_p)]_{m,k} = G\left(\frac{f_m+\hat{\epsilon}}{1+b_p} - f_k\right)$. Define a banded matrix $\mathbf{\Gamma}^D$ which keeps the $2D+1$ diagonals of $\mathbf{\Gamma}$, then the banded channel mixing matrix is

$$\mathbf{H}^D = \sum_{p=1}^{N_{\rm pa}} \xi_p \mathbf{\Lambda}(\bar{\tau}_p) \mathbf{\Gamma}^D(b_p). \tag{14}$$

2.3.1 Sparse Channel Representation Based on Overcomplete Dictionary

The channel matrix $\mathbf{H}^D$ has $K(2D+1) - D(1+D)$ entries, but can be specified by $N_{\rm pa}$ triple parameters of $\{\xi_p, \bar{\tau}_p, b_p\}$ [60]. The overcomplete dictionary for sparse channel estimation as described in [11] can be constructed, to transform (11) into a CS

problem. The path parameters $\{\bar{\tau}_p, b_p\}$ are discretized into uniformly spaced grids,

$$\bar{\tau}_p \in \left\{0, \frac{T}{\lambda_{\rm b} K}, \frac{2T}{\lambda_{\rm b} K}, \ldots, T_{\rm g}\right\} \tag{15}$$

$$b_p \in \left\{ -b_{\max}, -b_{\max} + \triangle b, \ldots, b_{\max}\right\} \tag{16}$$

where T/K is the sampling interval in baseband, $\lambda_{\rm b}$ is the oversampling factor, and $N_1 = \lambda_{\rm b} K T_{\rm g}/T$ tentative delays cover the channel delay spread; $b_{\max}$ covers the Doppler spread, and $\triangle b$ is the Doppler resolution, leading $N_2 = 2b_{\max}/(\triangle b) + 1$ tentative residual Doppler rates. Although $N_1 N_2$ candidate paths will be searched, the energy of most paths would be close to zero due to the characteristics of a sparse channel.

Define the vector $\boldsymbol{\xi}_i = [\xi_{1,i}, \ldots, \xi_{N_1,i}]^T$ to be the path gains with the same Doppler rate b_i, and stack $\boldsymbol{\xi}_i$ into a long vector as $\mathbf{x} = [\boldsymbol{\xi}_1^T, \ldots, \boldsymbol{\xi}_{N_2}^T]^T$. Denote the indices of pilot and null subcarriers within the signal band as $\{p_1, \cdots, p_{K_1}\}$ where K_1 is the total number of pilot and null subcarriers. Define a $K_1 \times K$ selector diagonal matrix $\boldsymbol{\Psi}$ with unit entry of $\boldsymbol{\Psi}[k, p_k] = 1$ for $k = 1, \cdots, K_1$, and zeros elsewhere. Define $\mathbf{z}_{\rm P} = \boldsymbol{\Psi}\mathbf{z}$, $\boldsymbol{\eta}_{\rm P} = \boldsymbol{\Psi}\boldsymbol{\eta}$, and

$$\mathbf{s}_{\rm P} = \begin{cases} \mathbf{s}[k], & k \in \mathcal{S}_{\rm P} \\ \\ 0, & k \in \mathcal{S}_{\rm N} \cup \mathcal{S}_{\rm D} \end{cases}. \tag{17}$$

Combining all $N_1 N_2$ candidate paths, the input-output relationship can be rewritten as a sparse representation form under the banded-ICI assumption,

$$\mathbf{z}_{\rm P} = \boldsymbol{\Psi}\left(\sum_{l=1}^{N_1}\sum_{i=1}^{N_2} \xi_{l,i} \boldsymbol{\Lambda}(\bar{\tau}_l)\boldsymbol{\Gamma}^D(b_i)\mathbf{s} + \boldsymbol{\eta}\right) \approx \mathbf{A}\mathbf{x} + \boldsymbol{\eta}_{\rm P} \tag{18}$$

where

$$\mathbf{A} = [\mathbf{\Psi}\mathbf{\Lambda}(\bar{\tau}_1)\mathbf{\Gamma}^D(b_1)\mathbf{s}_{\mathrm{P}}, \ldots, \mathbf{\Psi}\mathbf{\Lambda}(\bar{\tau}_{N_1})\mathbf{\Gamma}^D(b_{N_2})\mathbf{s}_{\mathrm{P}}]. \tag{19}$$

The sparse signal recovery algorithms, to be discussed in Section 2.3.2, can be used to estimate the path gain $\mathbf{x}$, based on which the banded channel mixing matrix $\mathbf{H}^D$ can be reconstructed according to (14).

2.3.2 Sparse Recovery Algorithms

Sparse recovery algorithms, which take advantage of the sparse structure of UWA channels, can be used for channel estimation through solving (18). Taking the L_q quasi-norm as a regularization term to control the solution sparsity, the sparse channel estimation problem in (18) can be reformulated as

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \ \frac{1}{2}\|\mathbf{z}_{\mathrm{P}} - \mathbf{A}\mathbf{x}\|_2^2 + \lambda\|\mathbf{x}\|_q^q. \tag{20}$$

For different choices of q, different L_q regularization problems are derived.

2.3.2.1 L_2 Algorithms - LSQR

Solving an L_2 problem equals to approximating the solution by minimizing the power of error,

$$\min_{\mathbf{x}} \ \frac{1}{2}\|\mathbf{z}_{\mathrm{P}} - \mathbf{A}\mathbf{x}\|_2^2 + \lambda\|\mathbf{x}\|_2^2, \tag{21}$$

but the solution can be not sparse with high probability. LSQR constructs an approximation by undergoing the bidiagonization process of Golun and Kahan [83]. LSQR

resembles the conjugate gradient method, but is more stable and reliable when **A** is ill conditioned.

2.3.2.2 L_0 Algorithms - OMP

L_0 penalty yields the most sparse solution, but it is NP-hard [15]. OMP can get the local optimal solution of L_0 problem with a low computational complexity,

$$\min_{\mathbf{x}} \|\mathbf{x}\|_0 \quad \text{s.t. } \|\mathbf{z}_\mathrm{P} - \mathbf{A}\mathbf{x}\|_2^2 \leq \delta. \tag{22}$$

Assuming that the observation vector $\mathbf{z}_\mathrm{P}$ is a linear combination of the columns of **A**, OMP reconstructs the sparse signal iteratively. At each iteration, OMP chooses one column from **A** that mostly resembles the residual vector, and then finds the solution $\mathbf{x}_n$ in the nth iteration by solving an LS problem with the combination of all n chosen column vectors [107].

2.3.2.3 L_1 Algorithms

Since (22) with L_0 penalty is an NP-hard problem, the approximation problem with L_1 penalty is often preferred, which turns (20) into a convex quadratic optimization problem,

$$\min_{\mathbf{x}} \ \frac{1}{2}\|\mathbf{z}_\mathrm{P} - \mathbf{A}\mathbf{x}\|_2^2 + \lambda\|\mathbf{x}\|_1^1. \tag{23}$$

Among the corresponding sparse recovery algorithms, considering that SpaRSA has shown good performance in [48], and that Nesterov, FISTA, and TwIST are the fast algorithms supported by Matlab toolboxes, we take them as the representative of L_1

solvers for performance comparison.

SpaRSA: SpaRSA is an iterative shrinkage/thresholding (IST) algorithm, which solves the second order approximation of (23),

$$\mathbf{x}_{n+1} \in \arg\ \min_{\mathbf{w}} \frac{1}{2}\|\mathbf{w}-\mathbf{u}_n\|_2^2 + \frac{\lambda}{\alpha_n}\|\mathbf{w}\|_1^1 \tag{24}$$

where $\mathbf{u}_n = \mathbf{x}_n + \frac{1}{\alpha_n}\mathbf{A}^H(\mathbf{z}_{\mathrm{P}} - \mathbf{A}\mathbf{x}_n)$. α_n is chosen by Barzilai-Borwein spectral method, so that $\alpha_n\mathbf{I}$ can mimic the Hessian matrix $\nabla^2(\frac{1}{2}\|\mathbf{z}_{\mathrm{P}} - \mathbf{A}\mathbf{x}\|_2^2)$ over the step just taken, leading accelerated convergence. Then the solution of (24) is

$$\mathbf{x}_{n+1} = \mathrm{soft}(\mathbf{u}_n, \frac{\lambda}{\alpha_n}) \tag{25}$$

where $\mathrm{soft}(\mathbf{u}, a) = \max(0, 1 - \frac{a}{\|\mathbf{u}\|})\mathbf{u}$. Continuation procedure can be used to accelerate the convergence speed [118].

Nesterov: Nesterov's Primal-Dual approach is a complex accelerated scheme, which solves the same problem in (24) as SpaRSA [82], but α_n is replaced by the Lipschitz constant $\alpha_n = \|\mathbf{A}\|_2^2$. To speed up the convergence, $\mathbf{u}_n$ becomes a linear combination of two vectors, where one is derived from the problem in (24), and the other from a subproblem which involves a weighted sum of all past gradients, resulting a convergence rate of n^2.

FISTA: FISTA is a faster IST algorithm with its convergence rate accelerated to n^2 [9]. Similar to Nesterov which combines the results of all previous iterations to speed up convergence, FISTA works on the two previous estimates directly, which

holds the computational expense nearly the same as Nesterov.

TwIST: TwIST is a combination of IST and IRS (iterative reweighted shrinkage) algorithms. It has the good denoising performance of IST scheme, while can tackle the ill-posed problem as efficiently as IRS. For TwIST, each iteration depends on the two previous estimates [13]. Its solution is

$$\mathbf{x}_{n+1} = (1-\zeta)\mathbf{x}_{n-1} + (\zeta-\beta)\mathbf{x}_n + \beta \cdot \text{soft}(\mathbf{u}_n, \lambda) \tag{26}$$

where ζ and β are the positive relaxation factors that control the convergence of the iteration.

2.3.2.4 $L_{1/2}$ Algorithm

$L_{1/2}$ regularization is a non-convex, non-smooth, and non-Lipschitz optimization problem,

$$\min_{\mathbf{x}} \ \frac{1}{2}\|\mathbf{z}_{\mathrm{P}} - \mathbf{A}\mathbf{x}\|_2^2 + \lambda\|\mathbf{x}\|_{1/2}^{1/2} \tag{27}$$

but has a fast solution due to the existence of the resolvent of gradient of $\|\mathbf{x}\|_{1/2}^{1/2}$ [124]. $L_{1/2}$ seems promising among L_q $(0 < q < 1)$ problems: when $q \in [\frac{1}{2}, 1]$, $L_{1/2}$ yields the best sparse solution; when $q \in [0, \frac{1}{2}]$, the performance is not significantly different.

The iterative solution of half thresholding algorithm $L_{1/2}$ based on a known sparsity κ (the number of non-zero entries) of $\mathbf{x}$ can be written as,

$$\mathbf{x}_{n+1} = \mathcal{H}_{\lambda_n\mu,\frac{1}{2}}(B_\mu(\mathbf{x}_n)) \tag{28}$$

where $B_\mu(\mathbf{x}) = \mathbf{x} + \mu\mathbf{A}^H(\mathbf{z}_\mathrm{P} - \mathbf{A}\mathbf{x})$, step size $\mu \in (0, \|\mathbf{A}\|_2^{-2}]$, and the half thresholding operator $\mathcal{H}_{\lambda\mu,\frac{1}{2}}(\mathbf{x})$ is defined as

$$\mathcal{H}_{\lambda\mu,\frac{1}{2}}(\mathbf{x}) = \begin{cases} \frac{2}{3}\|\mathbf{x}\|(1+\cos(\frac{2}{3}\pi - \frac{2\varphi_{\lambda\mu(\mathbf{x})}}{3})) & \|\mathbf{x}\| > \frac{\sqrt[3]{54}}{4}(\lambda\mu)^{\frac{2}{3}} \\ 0 & \text{otherwise} \end{cases} \tag{29}$$

where $\varphi_{\lambda\mu(\mathbf{x})} = a\cos(\frac{\lambda\mu}{8}(\frac{\|\mathbf{x}\|}{8})^{-\frac{3}{2}}))$. The corresponding near-optimal regularization parameter λ_n is expressed as

$$\lambda_n = \frac{\sqrt{96}}{9\mu}(\|B_\mu(\mathbf{x})\|_{\kappa+1})^{\frac{3}{2}} \tag{30}$$

where $\|B_\mu(\mathbf{x})\|_{\kappa+1}$ is the $(\kappa+1)$-th largest component in magnitude.

2.4 Data-driven Sparsity Learning

The sparse recovery algorithms discussed in Section 2.3.2 require the regularization parameter λ in L_1 and L_2, and sparsity κ in $L_{1/2}$, to be predefined in practical systems. However, due to time variation of UWA environments, constant regularization parameter λ and sparsity κ may not be appropriate all the time. Under-sized sparsity brings higher MSE, and degrades decoding performance. Over-sized sparsity not only results in overfitting, but also increases the computation complexity. Here, we propose a data-driven sparsity learning algorithm based on an LMMSE equalizer to select the regularization parameter λ, where golden section search is proposed to accelerate the learning process.

2.4.1 Data-driven Sparsity Learning based on an LMMSE Equalizer

Assume that the UWA channel does not change much during the transmission of a data burst with N_{b} OFDM blocks. Taking the first block in a data burst as a pilot block whose data symbols are known at the receiver, we propose to use the regularization parameter λ or sparsity κ tuned in the first block for channel estimation in the following blocks within this burst.

Remark 1. Note that if there is a preamble, the sparsity can be estimated based on the preamble. Otherwise, the first block will be used as the preamble, as done in this chapter.

The proposed data-driven sparsity learning algorithm uses the LMMSE equalizer from [108] to select the sparsity. The null subcarriers of the first OFDM block are used for noise variance estimation. The pilot subcarriers are used for channel estimation, and the data subcarriers are used for regularization parameter tuning. Take λ for example. The procedure is as follows.

Firstly the noise variance $\hat{\sigma}_{\mathrm{N}}^2$ is initially estimated based on measurements on the null subcarriers within the signal band, where the ambient and ICI noise are included,

$$\hat{\sigma}_{\mathrm{N}}^2 = \frac{1}{|\mathcal{S}_{\mathrm{N}}|} \sum_{m \in \mathcal{S}_{\mathrm{N}}} |z[m]|^2 . \tag{31}$$

Based on the sparse channel estimate $\hat{\mathbf{H}}^D$ obtained in Section 2.3.2, the observation on the mth subcarrier can be reformulated as

$$z[m] = \sum_{k=m-D}^{m+D} \hat{H}[m,k] s[k] + \tilde{\eta}[m] \tag{32}$$

where $\tilde{\eta}[m]$ now contains the error introduced in channel estimation.

The LMMSE equalizer, which is used to mitigate ICI and detect data symbols, can help to find the optimal regularization parameter λ. According to (32), stack all the observations, and we have

$$\mathbf{z} = \hat{\mathbf{H}}\mathbf{s} + \tilde{\boldsymbol{\eta}}. \tag{33}$$

Then the LMMSE estimate of $\mathbf{s}$ can be expressed as

$$\hat{\mathbf{s}} = \hat{\mathbf{H}}^H \left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H + \frac{\hat{\sigma}_{\mathrm{N}}^2}{\sigma_s^2}\mathbf{I} \right)^{-1} \mathbf{z} \tag{34}$$

where the mean and variance of $\mathbf{s}$ are defined as $E(\mathbf{s}) = \mathbf{0}$, $\Sigma_{\mathbf{s}} = \mathrm{Cov}(\mathbf{s}, \mathbf{s}) = \sigma_s^2\mathbf{I}$, and σ_s^2 is the average symbol energy. Define $\hat{\mathbf{h}}_m$ as the mth column of $\hat{\mathbf{H}}$ that relates to $s[m]$ directly. The LMMSE estimate of $s[m]$ can be given as [114]

$$\hat{s}[m] = \alpha[m]s[m] + \eta'[m] \tag{35}$$

where the equivalent noise $\eta'[m]$ is assumed to be Gaussian distributed $\eta'[m] \sim \mathcal{CN}(0, \sigma_{\eta'}^2[m])$, and

$$\alpha[m] = \hat{\mathbf{h}}_m^H \left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H + \frac{\hat{\sigma}_{\mathrm{N}}^2}{\sigma_s^2}\mathbf{I} \right)^{-1} \hat{\mathbf{h}}_m, \tag{36}$$

$$\sigma_{\eta'}^2[m] = \sigma_s^2(\alpha[m] - \alpha[m]^2). \tag{37}$$

In the first block where $s[m]$ is known in advance, $\hat{s}[m]$ is Gaussian distributed with $\hat{s}[m] \sim \mathcal{CN}(\alpha[m]s[m], \sigma_{\eta'}^2[m])$. The data-driven sparsity learning approach aims to minimize the objective function $J(\lambda)$, which is the average of the weighted mean-square error on all data subcarriers of the first block.

$$\lambda_{\text{opt}} = \arg\min_{\lambda} J(\lambda) = \arg\min_{\lambda} \frac{1}{|\mathcal{S}_{\mathrm{D}}|} \sum_{m \in \mathcal{S}_{\mathrm{D}}} \frac{|\hat{s}[m] - \alpha[m]s[m]|^2}{\sigma_{\eta'[m]}^2} \tag{38}$$

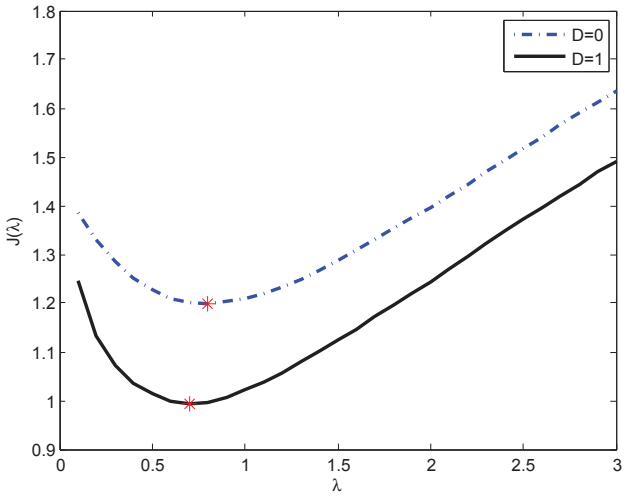


Figure 1: $J(\lambda)$ vs. λ, for $D = 0/1$ based on LMMSE from one training block, Julian date 300, SPACE08

Remark 2. For the ICI-ignorant receiver ($D = 0$), the equivalent criteria to select λ_{opt} based on the LMMSE equalizer would reduce to:

$$\lambda_{\text{opt}} = \arg\min_{\lambda} J(\lambda) = \arg\min_{\lambda} \frac{1}{|\mathcal{S}_{\text{D}}|} \sum_{m \in \mathcal{S}_{\text{D}}} \left| z[m] - \hat{H}[m,m]s[m] \right|^2, \qquad (39)$$

which amounts to minimizing the variance of the effective noise on data subcarriers. Since the performance based on the LMMSE equalizer outperforms that based on effective noise variance in the ICI-aware receiver, only the former one will be discussed in this chapter.

Figure 1 shows that the objective function $J(\lambda)$ has a convex shape with respect to the regularization parameter λ in the ICI-ignorant and the ICI-aware receivers based on the LMMSE equalizer. The optimal λ_{opt} that minimizes $J(\lambda)$ is marked by the star in Figure 1. Then the tuned λ_{opt} from the training block will be used to decode the following data blocks.

2.4.2 Golden Section Search

The data-driven sparsity learning approach aims to find the optimal value of λ_{opt} that minimizes the cost function (38). However, no analytical solution can be obtained by taking the derivative of (38). An exhaustive search of λ_{opt} within a preknown interval $\lambda \in [\lambda_{\min}, \lambda_{\max}]$ could be performed but is often computationally intensive. Leveraging on the convex property of the objective function as shown in Figure 1, we propose a golden-section search to find the desired λ with an affordable computational complexity. Even if there might be some small oscillations at some parts, it would not deteriorate the performance significantly unless the search process requires a very small step size [8].

The search interval of λ is critical. As [39] indicates, when λ is close to zero, there would be no sparse solution of (20). While for $\lambda \geq \|\mathbf{A}^H \mathbf{z}_{\text{P}}\|_\infty$, the optimal solution would be $\hat{\mathbf{x}} = 0$. Thus, the optional interval of λ is

$$\lambda \in (0, \|\mathbf{A}^H \mathbf{z}_{\text{P}}\|_\infty). \tag{40}$$

For the $L_{1/2}$ case, the sparsity κ equals to the estimated number of paths $\hat{N}_{\text{pa}}$. The lower boundary of $\hat{N}_{\text{pa}}$ is 1, which is the minimal positive integer. The upper boundary can be determined by the number of observations N_{obs} in one OFDM block, which shows the most number of non-zeros elements of unknowns $\mathbf{x}$ that can be recovered in the sparse-domain. Hence, we have

$$\hat{N}_{\text{pa}} \in [1, N_{\text{obs}}] \tag{41}$$

where $N_{\text{obs}} = K_{\text{P}} + K_{\text{N}}$, the total number of pilot and null subcarriers.

Take λ for example. Algorithm 1 shows how golden section search works. The procedure would be the same for the $L_{1/2}$ case.

Algorithm 1 : Golden Section Search

Initialization:
  Set the golden ratio: $\gamma = \frac{1+\sqrt{5}}{2}$;
  Set the initial search interval of λ: $[\lambda_{\min}, \lambda_{\max}]$;
  Define the current interval length: $L_{\text{cur}} = \lambda_{\max} - \lambda_{\min}$;
  Define the tolerant interval as the stopping criteria: L_{tol};
repeat
  Select λ_1 and λ_2 within interval $[\lambda_{\min}, \lambda_{\max}]$ for evaluation:

$$\lambda_1 = \lambda_{\min} + (1-\gamma)L_{\text{cur}}$$
$$\lambda_2 = \lambda_{\max} - (1-\gamma)L_{\text{cur}}$$

  Estimate the channel $\hat{\mathbf{H}}(\lambda_1)$, and $\hat{\mathbf{H}}(\lambda_2)$. Evaluate $J(\lambda_1)$ and $J(\lambda_2)$.
  if $J(\lambda_1) < J(\lambda_2)$ **then** $\lambda_{\max} = \lambda_2$;
  else $\lambda_{\min} = \lambda_1$;
  end if
  $L_{\text{cur}} = \lambda_{\max} - \lambda_{\min}$.
until $L_{\text{tol}} > L_{\text{cur}}$
Output: $[\lambda_{\text{opt}}, \hat{\mathbf{H}}(\lambda_{\text{opt}})] = \min_{\lambda} \ (J(\lambda_{\min}), J(\lambda_{\max}))$

Finally, the optimal regularization parameter λ_{opt} and the corresponding channel matrix $\hat{\mathbf{H}}(\lambda_{\text{opt}})$ can be found by $\lceil 1.44 \times \log_2(\frac{\lambda_{\max}-\lambda_{\min}}{L_{\text{tol}}}) \rceil$ iterations during the search process.

Note that the golden section search algorithm will not be used in OMP. By increasing the number of iterations, OMP finds solutions with more non-zero entries. The best OMP solution is determined by the data-driven approach in (38).

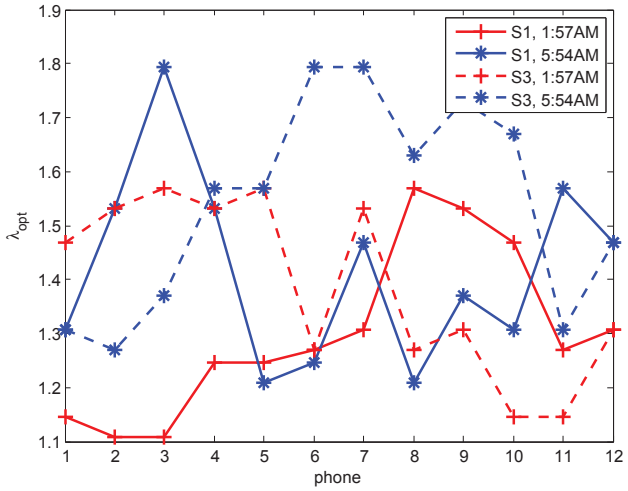


Figure 2: The tuned λ_{opt} on different phones from blocks at different time, Julian date 300, SPACE08

2.4.3 Multichannel Combination

For an array with multiple hydrophones, different hydrophones often have different channels. The optimal regularization parameter may have different optimal values λ_{opt} across hydrophones. Figure 2 shows the result from the 2008 Surface Processes and Acoustic Communications Experiment (SPACE08) experiment, that the tuned λ_{opt} changes with the hydrophone, the transmission time, and the distance S1 and S3 between transmitter and receivers. It is necessary to train λ separately. For the rth data block of the vth hydrophone, the effective noise variance on pilots $\mathcal{S}_{\text{P}}$ after channel estimation is estimated by

$$\hat{\sigma}^2_{r,v} = \frac{1}{|\mathcal{S}_{\text{P}}|} \sum_{m \in \mathcal{S}_{\text{P}}} \left| z_{r,v}[m] - \sum_{k=m-D}^{k=m+D} \hat{H}_{r,v}[m,k] s_{r,v}[k] \right|^2 \tag{42}$$

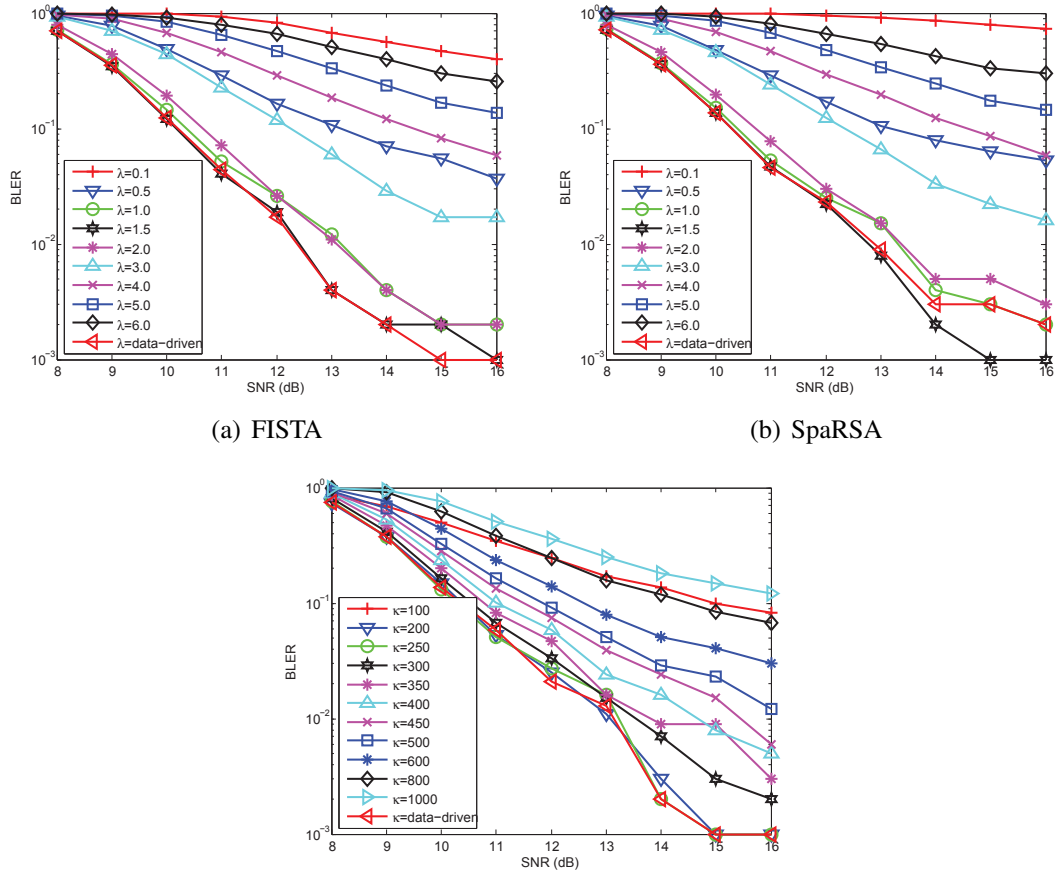
where the residual ICI, channel estimation error and the ambient noise are included. Hydrophone combining can be carried out as in [110] after the frequency measurements are weighted by the factor $\frac{1}{\sqrt{\hat{\sigma}^2_{r,v}}}$.

2.5 Simulation Results

A single-input single-output (SISO) OFDM system is considered for simulation, with center frequency $f_{\mathrm{c}} = 13$ kHz, bandwidth $B = 9.77$ kHz, symbol duration $T = 104.86$ ms, and guard interval $T_g = 24.6$ ms. The OFDM system has a total of $K = 1024$ subcarriers, out of which 96 are null subcarriers and 256 are pilot subcarriers. Among the null subcarriers, 24 are placed on the edges of signal band for band protection, and the rest 48 subcarriers are equi-spaced in the middle of signal band. 256 pilot subcarriers are uniformly distributed among the signal band. For the ICI-aware receiver, 96 data subcarriers adjacent to the middle null subcarriers and existing pilots, are taken as extra pilot subcarriers for ICI estimation [11]. The remaining data subcarriers are encoded using an LDPC code with rate $1/2$, and modulated with 16-QAM constellation. The pilot symbols are modulated with QPSK constellation, with 1.5 times of power than that of data.

The simulated sparse channel has 15 discrete paths. The inter-arrival time of paths is exponentially distributed with mean of 1 ms, resulting a 15-ms channel delay spread on average. The Doppler rate of each path is independently distributed $a_p = v_p/c$, where v_p is the relative speed between the transmitter and the receiver with the standard

deviation of 0.2 m/s, and c is the sound speed. The amplitude of each path is Rayleigh distributed, whose average power decreases exponentially with delay.



(a) FISTA (b) SpaRSA

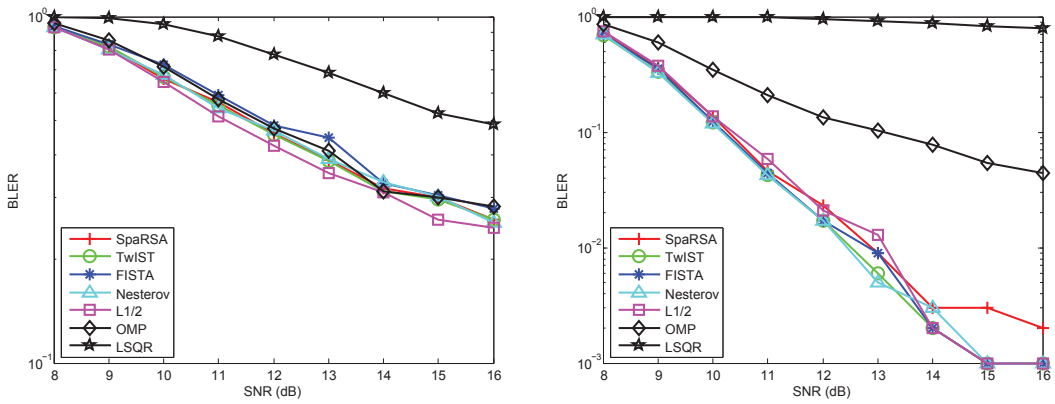
(c) $L_{1/2}$

Figure 3: BLER vs. SNR, SISO with ICI-aware receivers, 16-QAM.

We generate 100 OFDM packets, with each packet consisting of 10 OFDM blocks, resulting 1000 blocks in total. We assume that the channel does not change within each packet transmission. The spectral efficiency α and the data rate R for the ICI-aware receiver are [11]

$$\alpha = \frac{T}{T+T_g} \cdot \frac{336-96}{1024} \cdot \log_2 16 = 0.76 \text{ bits/s/Hz}, \tag{43}$$

$$R = \alpha B = 7.42 \text{ kb/s}. \tag{44}$$



(a) ICI-ignorant receivers ($D = 0$) (b) ICI-aware receivers ($D = 1$)

Figure 4: Data-driven sparsity learning, BLER vs. SNR, SISO, 16-QAM.

The corresponding spectral efficiency and data rate for the ICI-ignorant receiver would be $\alpha = 1.06$ bits/s/Hz and $R = 10.39$ kb/s [11].

The oversampling factor λ_{b} of the delay grid in the overcomplete dictionary is set to be 2. Since the covered channel delay spread by the channel estimator is equivalent to the guard interval, there are $N_1 N_2 = \lambda_{\mathrm{b}} T_{\mathrm{g}} B = 480$ unknowns that need to be estimated for the ICI-ignorant receiver by assuming no Doppler spread $N_2 = 1$, and there are $N_1 N_2 = 7200$ unknowns for the ICI-aware receiver by assuming $N_2 = 15$ Doppler values within an interval $[-5 \cdot 10^{-4}, 5 \cdot 10^{-4}]$. The span of golden section search is set to be $[0.1, 8.0]$, with the search span of termination to be less than 0.2. The tolerance for L_q algorithms on $\mathbf{x}$ is 1e-4, with maximal iteration to be 50.

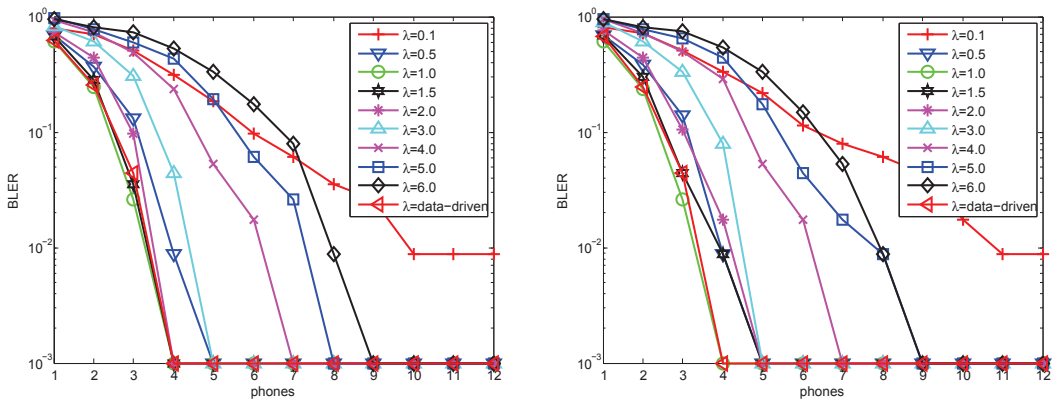
We take SpaRSA, FISTA, and $L_{1/2}$ under $D = 1$ as representatives to show the performance of the sparse recovery algorithms with data-driven sparsity learning. As shown in Figure 3(a), 3(b), and 3(c), the prefixed values of λ are 0.1, 0.5, 1.0, 1.5, 2.0, 3.0, 4.0, 5.0, and 6.0, and the prefixed sparsity $\hat{N}_{\mathrm{pa}}$ are 100, 200, 300, 350, 400,

450, 500, 600, 800 and 1000. SpaRSA, FISTA, and $L_{1/2}$ can achieve nearly the best performance compared to the case of fixed λ and $\hat{N}_{\rm pa}$ for $D = 1$ with $\lambda_{\rm opt} = 1.0$ and 1.5, and $\hat{N}_{\rm pa,opt} = 200$ and 250. The result demonstrates the importance of selecting appropriate λ and $\hat{N}_{\rm pa}$, and verifies the effectiveness of the data-driven approach. The under-sized and over-sized λ and $\hat{N}_{\rm pa}$ will degrade the performance of the L_q algorithms.

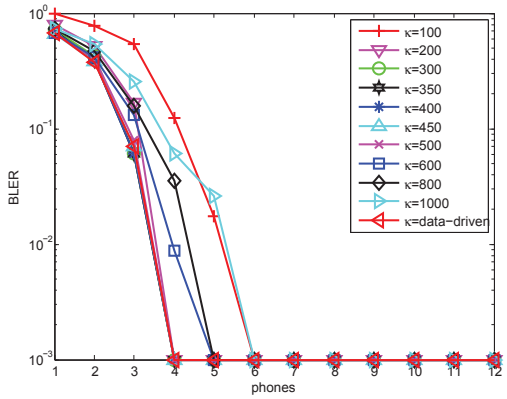
Figure 4 shows the performance of the L_q algorithms with data-driven sparsity learning approach. We can see that the ICI-aware receivers considerably outperform the ICI-ignorant receivers. LSQR performs the worst due to the model mismatch. The $L_{1/2}$, and L_1 algorithms have similar performance.

2.6 Experimental Results - SPACE08 Experiment

To evaluate the performance of the data-driven sparsity learning approach, the data collected from the SPACE08 experiment are used. The SPACE08 experiment was conducted off the coast of Martha's Vineyard, MA, from Oct. 14 to Nov. 1, 2008, where the water depth was about 15 meters. The transmitter and six receivers were anchored at different locations of the sea bottom. Each receiver was a 12-element array with elements spaced by 0.1 meter, resulting a single-input multi-output (SIMO) system. We consider two receivers labeled as S1 and S3 which were 60 meters and 200 meters away from the transmitter, respectively. The recorded data from Julian Dates 300 are considered, since this day suffered the toughest weather condition during the experiment.



(a) FISTA (b) SpaRSA

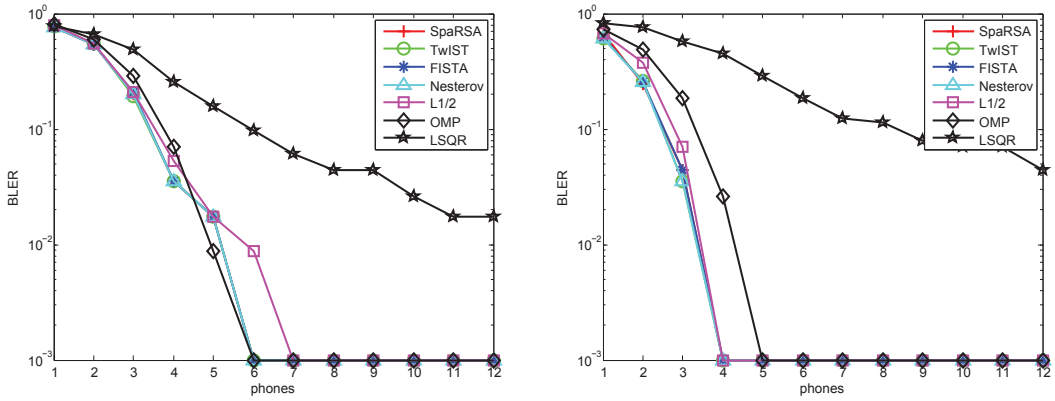


(c) $L_{1/2}$

Figure 5: SIMO with ICI-aware receiver, 16-QAM, Julian date 300, SPACE08-S1 (60 m)

In the SPACE08 experiment, the transmitter sent 20 consecutive OFDM blocks every 2 hours. In total 12 data files were saved each day. On Julian Date 300, 5 files recorded during the afternoon were severely distorted, therefore only the remaining data files are used to test the performance. The parameter setting in this experiment is the same as that in simulation.

Figures 5(a), 5(b) and 5(c) compare the performance between data-driven and fixed-sparsity FISTA, SpaRSA, and $L_{1/2}$ in the ICI-aware receiver ($D = 1$). The prefixed value of λ and sparsity $\hat{N}_{\mathrm{pa}}$ are the same as that in simulation. Different λ's

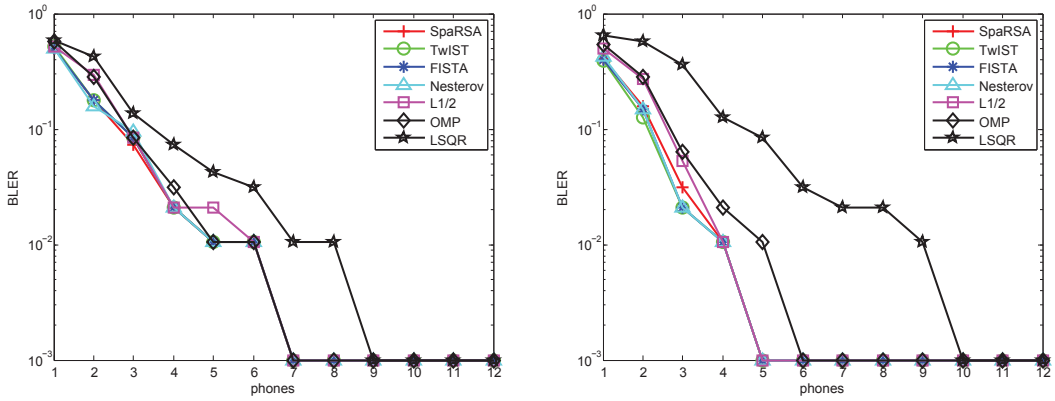


(a) ICI-ignorant receivers ($D = 0$) (b) ICI-aware receivers ($D = 1$)

Figure 6: Data-driven sparsity learning, SIMO, 16-QAM, Julian date 300, SPACE08-S1 (60 m)

lead to quite different performance of FISTA and SpaRSA, which indicates the necessity to select a proper value of λ. The BLER curves of $L_{1/2}$ are tighter during the span of prefixed $\hat{N}_{\mathrm{pa}}$, which suggests $L_{1/2}$ is insensitive to $\hat{N}_{\mathrm{pa}}$ in this experiment. We can see that FISTA with data-driven sparsity approximates the best performance with fixed λ =1.0 and 1.5. SpaRSA with data-driven sparsity presents the same best BLER performance as the fixed $\lambda = 1.0$. $L_{1/2}$ with data-driven sparsity approximates the best with $\hat{N}_{\mathrm{pa}} = 200, 300, 350, 400, 450, 500$. In short, the three algorithms with data-driven sparsity learning approximate the best performance of the fixed λ or $\hat{N}_{\mathrm{pa}}$, which demonstrates the validity of the data-driven method.

Figure 6 shows the BLER performance of the ICI-ignorant receiver and the ICI-aware receiver with an increasing number of phones for S1, where the data-driven approach is used to select the proper regularization parameter λ and sparsity $\hat{N}_{\mathrm{pa}}$. As Figure 6(a) and 6(b) demonstrate, we can see that the ICI-aware receivers outperform the ICI-ignorant receivers. LSQR fails to decode the blocks due to model mismatch.



(a) ICI-ignorant receivers ($D = 0$)

(b) ICI-aware receivers ($D = 1$)

Figure 7: Data-driven sparsity learning, SIMO, 16-QAM, Julian date 300, SPACE08-S3 (200 m)

OMP and all the listed L_1 algorithms have better performance than $L_{1/2}$ algorithms when $D = 0$. However, all the L_1 and $L_{1/2}$ algorithms have the same performance when $D = 1$, which is better than that of OMP.

Figure 7 demonstrates the BLER performance of the ICI-ignorant receiver and the ICI-aware receiver with an increasing number of phones for S3, where the data-driven sparsity learning method is included in all the listed L_q algorithms. With LSQR, the ICI-ignorant receiver has better performance than the ICI-aware receiver, since the solution of LSQR is not sparse with high probability, which degrades the performance of the ICI-aware receiver which has more variables. With all other L_q algorithms, the ICI-aware receivers outperform the ICI-ignorant receivers. For both $D = 0$ and $D = 1$, SpaRSA, TwIST, FISTA, Nesterov, and $L_{1/2}$ have the best performance, much better than LSQR, while OMP is worse than L_1 and $L_{1/2}$ only for $D = 1$.

2.7 Conclusions

This chapter presented a data-driven sparsity learning approach based on an LMMSE equalizer to select a proper regularization parameter in OFDM systems. The golden section search was employed to accelerate the sparsity learning process. The block error rates of several different L_q algorithms were compared in the ICI-ignorant and the ICI-aware OFDM receivers. Simulation and experimental results showed that the half thresholding algorithm and the four BP solvers: SpaRSA, FISTA, Nesterov, and TwIST have nearly the same performance, which outperform the OMP algorithm, and the LSQR performs the worst. The data-driven sparsity learning approach helped to achieve nearly the same performance as that of the best fixed regularization parameter. We conclude that L_1 and $L_{1/2}$ sparse recovery algorithms based on data-driven sparsity learning are appealing choices in underwater OFDM systems.

Estimation of the underwater acoustic channel lays the foundation for secret key generation in underwater systems as described in the next chapter.

Chapter 3

Channel Frequency Response Based Secret Key Generation in Underwater Acoustic Systems

3.1 Introduction

Security has attracted great attention in recent years, due to the system vulnerabilities to malicious attacks [25, 26, 33, 81, 93, 142, 143]. The broadcast nature of wireless medium allows an attacker to eavesdrop the signals in the physical channel easily. It becomes a major concern to have shared secret keys among wireless sensor network (WSN) users to secure the private data [26, 55]. However, the public key infrastructure mechanisms are not practical for sensor networks since they need a certification authority, and the key predistribution schemes are not suitable for large-scale networks [100]. One area of active research is on dynamic key generation at the physical layer to provide secure communications for wireless systems [81, 100].

3.1.1 Key Generation in Wireless Radio Communications

Based on the reciprocity of the wireless channels between two legitimate users, various key generation protocols have been explored in wireless radio communications.

- The power variation of received signal strength (RSS) has been adopted for key generation in flat fading channels. The received signal strength indicators (RSSI) for many off-the-shelf wireless devices can be easily assessed. Smart antenna with beam-forming technique is used to create artificially fluctuant channels by adjusting the reactance randomly, leading independent RSSI for key generation [3]. A level-crossing algorithm with one-bit quantization to extract keys from the RSSI of correlated Rayleigh fading wireless channels is proposed in [78]. A multi-bit quantization of the RSSI can increase the secret key rates [128]. The framework in [85] uses interpolation within the coherence time to deal with the nonsimultaneous measurements of RSSI. Both the absolute amplitude and fading trend of RSSI are multi-bit quantized to address group secret key generation in star and chain topologies [68].

- The dominant channel taps of a channel impulse response (CIR) can be used as the randomness source for key generation. The complex channel coefficients are employed to extract secret keys by taking advantage of the multipath fading randomness [70]. The impact of the channel sparsity and the correlation between the main and eavesdropping channels on secret key capacity was studied

in [31], and the secret key capacity with/without eavesdropper were presented. The phase information of multipath was considered for key generation in [38], and the optimal guard intervals were derived to separate quantization regions.

- Multicarrier modulation, such as orthogonal frequency-division multiplexing (OFDM), is widely used in broadband communication systems. It can provide higher secrecy key rates by utilizing the channel frequency response (CFR). The key bits were quantized from the channel response of each individual subcarrier in [135]. As shown in [67, 120, 122, 127], the key bits can be quantized across all the subcarriers. An adaptive key generation approach was proposed in [127] based on the RSS of subcarriers in an OFDM system, where Discrete Cosine Transformation (DCT) was used to reduce the redundancy of the measured RSS and inverse DCT was used for RSS reconstruction, and adaptive multi-level quantization was carried out by exchanging parity information. In [120], both the real and imaginary parts of CFRs were used for key generation, where the original and conjugate of the received probing signals were exchanged for channel estimation. To achieve a higher secret rate, a Channel Gain Complement (CGC) assisted secret key generation protocol was proposed in [67] based on the fine-grained channel frequency response in an OFDM system, where the non-reciprocal components of CFRs were transmitted to enhance the correlation. The work in [122] proposed a fast secret key extraction protocol named KEEP based on the amplitude of CFRs, where the universal hash functions were used

to validate the consistency of keys, and the correlation of near-by subcarriers was eliminated by key combination after random bit-selection. The precoding matrix index (PMI)-based secret key generation with a rotation matrix was proposed for MIMO-OFDM systems in [119], where the randomly generated keys were embedded in transmitted signals as the index of the best procoding matrix, and the keys from both sides were exchanged secretly.

3.1.2 Scope and Contributions

In this chapter, we study dynamic key generation at the physical layer to provide secure underwater acoustic (UWA) communications. The research topics in underwater acoustic systems often lag behind the counterparts in wireless radio systems, however, there exists large room for exploration, due to the fundamental difference of underwater acoustic channels from radio channels. Due to the slow speed of sound in water, 1500 m/s versus the speed of light $3 \cdot 10^8$ m/s, the underwater acoustic channel is characterized of large propagation delay, low bandwidth, and severe Doppler effects due to the platform motion and media instability. We are motivated to investigate whether the physical layer techniques developed for radio channels are applicable to underwater acoustic systems.

Note that the importance of security concerns in underwater acoustic systems have been articulated in recent overview papers [33,62]. However, up to now only one work has investigated the secret key generation in UWA channels by exploring RSSI [74].

The contributions of this chapter are as follows.

1) We present a secret key generation protocol, which exploits the channel frequency response of OFDM systems in UWA channels. Leveraging the detailed channel information in the frequency domain, the proposed approach will greatly speed up the key generation process relative to RSSI based approaches [74] as more bits are generated in each round of message exchange.

   We have implemented part of the protocol in lake tests. By analyzing the collected data sets, we verify the correlation between mutual channels, and validate the effectiveness of the key generation approach.

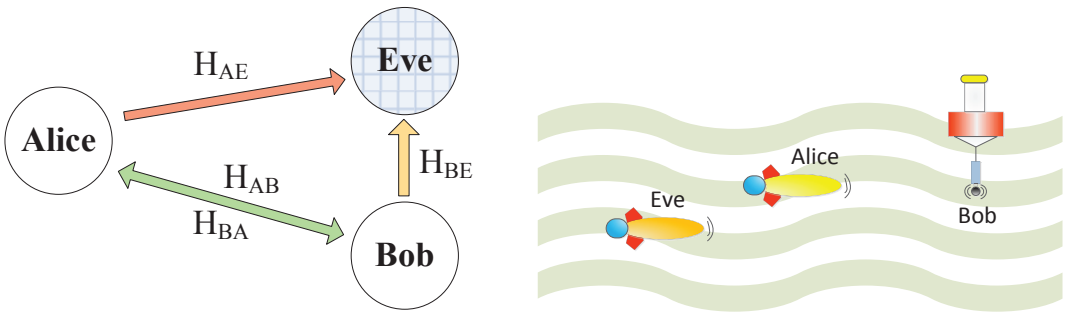
2) Based on the lake test results, we further improve the key generation protocol in UWA systems, by introducing the adaptive pilot signalling module to increase the correlation and the block-sliced key verification module to deal with channel dynamics. The simulation results show the feasibility of higher practical key generation rate. To our knowledge, the concept of adaptive pilot signalling has not been explored in the literature.

The rest of the chapter is organized as follows. Section 3.2 describes the system model and the secret key generation protocol using fixed pilots. Section 3.3 presents the lake test results. Section 3.4 discusses the improved secret key generation protocol utilizing adaptive pilots for signalling in details. Simulation results are provided in Section 3.5. Finally, we draw conclusions in Section 3.6.

Notation: Bold lower case letters and upper case letters denote column vectors and matrices, respectively. $(\cdot)^T$, $(\cdot)^*$ and $(\cdot)^H$ denote transpose, conjugate, and Hermitian transpose, respectively. $\mathcal{CN}(\cdot)$ denotes a random variable that follows complex Gaussian distribution. $\lfloor \cdot \rfloor$ denotes the floor function. $x[m]$ denotes the mth element of vector $\mathbf{x}$, and $H[m]$ denotes the mth element of the main diagonal of matrix $\mathbf{H}$. $\mathrm{E}\{\cdot\}$ denotes the expectation of a random variable.

3.2 System Description

The system configuration is shown in Fig. 8(a). Two nodes, Alice and Bob, aim to establish a secret key. Eve is the adversary who listens to the communications between Alice and Bob passively, and hopes to extract the same key. Fig. 8(b) illustrates a relevant scenario in an underwater network, where Bob acts as a data collection center and Alice, an autonomous underwater vehicle (AUV), collects data samples to be sent back to Bob. Eve is another AUV who wants to intercept the data from Alice by listening to the underwater acoustic transmissions between Alice and Bob.



(a) Node topology for key generation (b) An illustration in an underwater network

Figure 8: System configuration

3.2.1 System Model

Alice and Bob use the zero-padded OFDM block as the probing signal for channel estimation [52]. Define $z[k]$ as the frequency-domain measurement on the kth subcarrier f_k, $s[k]$ as the transmitted symbol on f_k, and $H[k]$ as the corresponding channel response in the frequency domain. The frequency-domain channel input-output relationship is

$$z[k] = H[k]s[k] + \eta[k], \quad k = -\frac{K}{2}, \ldots, \frac{K}{2} - 1 \tag{45}$$

where K is the number of subcarriers and is assumed to be even, and $\eta[k]$ contains the ambient noise and intercarrier interference (ICI) [52]. Using the matrix-vector notation, the compact form of (45) is

$$\mathbf{z} = \mathbf{H}\mathbf{s} + \boldsymbol{\eta}, \tag{46}$$

where $\mathbf{z}$, $\mathbf{s}$ and $\boldsymbol{\eta}$ denote the measurements from all subcarriers, transmitted symbols and noise vector respectively, and $\mathbf{H}$ is a diagonal matrix with $H[k]$ being its kth diagonal element.

As Fig. 8(a) shows, if Alice and Bob exchange the probing signals in turn, they would get the noisy observations

$$\mathbf{z}_{\mathrm{A}} = \mathbf{H}_{\mathrm{BA}}\mathbf{s}_{\mathrm{B}} + \boldsymbol{\eta}_{\mathrm{A}}, \tag{47}$$

$$\mathbf{z}_{\mathrm{B}} = \mathbf{H}_{\mathrm{AB}}\mathbf{s}_{\mathrm{A}} + \boldsymbol{\eta}_{\mathrm{B}}, \tag{48}$$

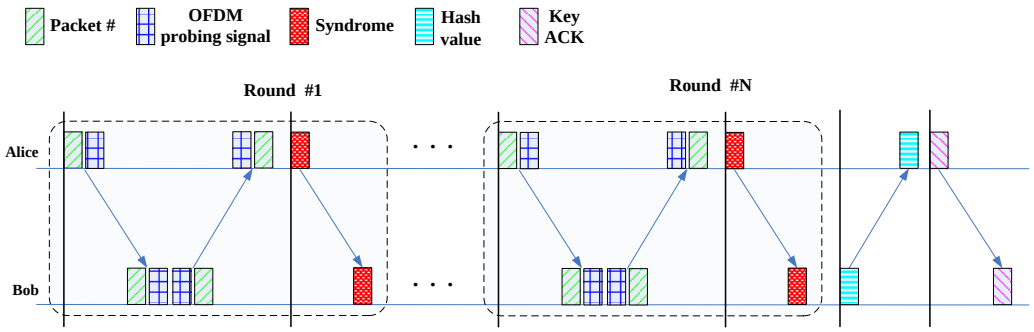


Figure 9: Secret key generation protocol using fixed pilots

where $\mathbf{H}_{\mathrm{BA}}$ is the channel matrix from Bob to Alice, and $\mathbf{H}_{\mathrm{AB}}$ from Alice to Bob. And Eve will observe

$$\mathbf{z}_{\mathrm{E}} = \mathbf{H}_{\mathrm{AE}}\mathbf{s}_{\mathrm{A}} + \boldsymbol{\eta}_{\mathrm{E}}, \tag{49}$$

$$\mathbf{z}'_{\mathrm{E}} = \mathbf{H}_{\mathrm{BE}}\mathbf{s}_{\mathrm{B}} + \boldsymbol{\eta}'_{\mathrm{E}}, \tag{50}$$

where $\mathbf{H}_{\mathrm{AE}}$ and $\mathbf{H}_{\mathrm{BE}}$ are the channels from Alice and Bob to Eve respectively. Since Eve stays multiple-wavelengths away from Alice and Bob[1] , she experiences different multipath channels, leading independent channel measurements.

3.2.2 Secret Key Generation Protocol

The secret key generation protocol used in lake tests is shown in Fig. 9. The description here is based on the used AquaSeNT OFDM modem [4], where three existing functionalities are called by the higher-layer protocol. First, the modem can send out a message using its data transmission mode with its own proprietary data processing

[1]The sound speed in water c is around 1500 m/s. For an acoustic modem with a center frequency at e.g., $f_{\mathrm{c}} = 10$ kHz and $f_{\mathrm{c}} = 20$ kHz, the wavelength is $\lambda = c/f_{\mathrm{c}} = 0.15$ m and $\lambda = 0.075$ m, respectively. Hence, this condition can be easily met in underwater acoustic systems when Eve is at least one meter away from Alice and Bob.

algorithms [4]. Second, the modem can play a pre-loaded arbitrary waveform using its waveplay function. Third, the modem can record the incoming signal once properly configured by a command. The procedure is as follows.

1) Alice first sends out a short message that contains the packet number, using the data transmission mode of the modem. Then she plays a known probing signal (for example, one fixed OFDM block in our tests) using the waveplay function of the modem. Once Bob has decoded the packet number correctly and receives the probing signal from Alice completely, he replies to Alice with the same OFDM probing signal immediately, and then the corresponding packet number he decoded. The packet number here is used for Alice and Bob to pair the OFDM probing signal due to the packet loss. Bob sends the packet number after the probing signal, to reduce the interval between the probing signals and provide the highest correlation between mutual channels.

2) Alice quantizes her observation of the underwater acoustic channel in the frequency domain, and generates the keys herself. Then she sends the syndrome to Bob based on the error correction code they predefine, aiming to help Bob recover the sequences that Alice observed. Bob quantizes his channel observation, then he extracts the keys with the help of the quantized channel frequency response available and the received syndrome. Step 1) and step 2) will repeat N times, until the desired length of keys can be extracted.

3) Bob sends the hash value to Alice where the generated keys are taken as the source of the hash function. Alice generates another hash value with the same hash function, and compares it with the value from Bob.

4) If the hash values of Alice and Bob are equal, the secret keys are regarded as matched and a Key Acknowledgement signal is transmitted to Bob.

3.2.3 Channel Estimation

Channel estimation is carried out based on the received data corresponding to the probing signal. We adopt the block fading assumption here, which means that the UWA channel remains quasi-static or slowly varying during probing in each round, but becomes independent from round to round. For this reason, we drop the index for the signal probing at different rounds. For each received probing signal, proper Doppler compensation is still needed to compensate the effect due to platform motion and medium instability. After Doppler compensation, the equivalent channel at the baseband can be represented as [52]

$$h(\tau) = \sum_{p=1}^{N_{\text{pa}}} \xi_p \delta\left(\tau - \tau_p\right), \tag{51}$$

where N_{pa} is the number of paths, ξ_p and τ_p are the amplitude and delay of the pth path, respectively. The channel frequency response of the kth subcarrier can be expressed as

$$H[k] = \sum_{p=1}^{N_{\text{pa}}} \xi_p e^{-j2\pi \frac{k}{T} \tau_p}. \tag{52}$$

Based on the channel model, sparse recovery algorithms with data-driven sparsity learning descripted in Chapter 2 are used to estimate the channel frequency response.

3.2.4 Channel Quantization

Quantization converts channel measurements into a binary bit stream; see e.g., [43, 131] on the descriptions of different quantization methods used for key generation. In this chapter, we focus on the quantization method based on the cumulative distribution function (CDF).

The channel frequency responses of successive frequencies may have high correlation, resulting long runs of zeros or ones after quantization. To reduce the correlation, we only select parts of the equal-spaced frequency response. Suppose that M frequencies $\{f_{p_1}, \cdots, f_{p_M}\}$ are selected, the used frequency measurements are $\{H[p_1], \cdots, H[p_M]\}$, where $p_1, \cdots, p_M$ are the indexes of the subcarriers.

Different from [67,122] which estimate the mean and variance of the amplitudes of CFR samples in a time sequence, we estimate the mean and variance of the amplitudes of CFRs across subcarriers. Then the mean and variance of the amplitudes of CFR are estimated as:

$$\mu_{\mathrm{H}} = \frac{1}{M}\sum_{i=1}^{M} |H[p_i]| \tag{53}$$

$$\varepsilon_{\mathrm{H}}^2 = \frac{1}{M-1}\sum_{i=1}^{M} (|H[p_i]| - \mu_{\mathrm{H}})^2 \tag{54}$$

The multi-bit CDF based quantization is used to quantize the amplitude of CFR into binary bits, where the threshold of different quantization intervals is set based on the

CDF of the amplitudes of CFR. Suppose we would like to extract t bits per measurement, then the amplitude of each subcarrier will be divided into 2^t equally likely regions. The CDF of $|H[k]|$ is defined as $F(x) = P(|H(k)| < x)$. The lth threshold to space different intervals can be determined by the inverse of the CDF,

$$q_l = F^{-1}\left(\frac{l}{2^t}\right), \quad l = 1, \cdots, 2^t - 1 \tag{55}$$

$$q_0 = -\infty, \qquad q_{2^t} = \infty. \tag{56}$$

Gray coding is constructed and mapped to different intervals. If $|H[k]|$ falls into the lth interval $[q_{l-1}, q_l)$, then the corresponding t-bit code will be used as the extracted bits. As in [67, 68], we adopt the Gaussian CDF for the quantizer, i.e., assuming that the CFR amplitudes follow the Gaussian distribution $|H[k]| \sim \mathcal{N}(\mu_{\mathrm{H}}, \varepsilon_{\mathrm{H}}^2)$. Note that only one-bit and two-bit quantizers are used in this chapter, where for the one-bit quantizer, the CFR amplitudes are simply compared against the mean value.

3.2.5 Key Reconciliation

Let $\mathbf{y}_{\mathrm{A}}$ and $\mathbf{y}_{\mathrm{B}}$ denote the binary codewords obtained at Alice and Bob, respectively, from their quantized versions of the channel frequency response. Due to noise and channel time variation, these two codewords are not identical. A reconciliation process can be carried out by error correction coding along the principle of Slepian-Wolf coding [59]. Assume a linear block code such as BCH(n, m) is used, where n is the length of codeword and m is the length of information word. If the length of $\mathbf{y}_{\mathrm{A}}$ and $\mathbf{y}_{\mathrm{B}}$ is larger than n, the bit sequences used for key extraction are collected in an

interleaving manner to make the length of each subset equals to n, and then cascade the bits of each subset to get the final key. As an example where the length of $\mathbf{y}_{\mathrm{A}}$ is n, the process is as follows.

1) Alice and Bob have an agreement on the BCH(n, m) code. They share the same 2^m information words of length m, $\{\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{2^m-1}\}$, the corresponding code words of length n, $\{\mathbf{c}_0, \mathbf{c}_1, \cdots, \mathbf{c}_{2^m-1}\}$, the generation matrix $\mathbf{G}$ and parity check matrix $\mathbf{P}$.

2) Alice calculates the syndrome $\mathbf{s}_{\mathrm{A}}$ of length $n - m$ based on her observation $\mathbf{y}_{\mathrm{A}}$. The syndrome can be obtained by $\mathbf{r}_{\mathrm{A}} = \mathbf{y}_{\mathrm{A}}\mathbf{P}^T$, or the coset leader $\mathbf{e}_{\mathrm{A}}$ with $\mathbf{r}_{\mathrm{A}} = \mathbf{e}_{\mathrm{A}}\mathbf{P}^T$. The key is the corresponding information word $\hat{\mathbf{b}}_{\mathrm{A}}$ generated by Alice

$$\hat{\mathbf{b}}_{\mathrm{A}} = \arg\min_{\mathbf{b}} \|\mathbf{y}_{\mathrm{A}} - \mathbf{b}\mathbf{G}\|, \tag{57}$$

and

$$\mathbf{e}_{\mathrm{A}} = \mathbf{y}_{\mathrm{A}} - \hat{\mathbf{b}}_{\mathrm{A}}\mathbf{G}. \tag{58}$$

3) Alice sends the helper information $\mathbf{r}_{\mathrm{A}}$ to Bob through the public channel. The effect of sending $\mathbf{r}_{\mathrm{A}}$ is equivalent to $\mathbf{e}_{\mathrm{A}}$, but $\mathbf{r}_{\mathrm{A}}$ is preferred due to its shorter length. Though Eve can overhear $\mathbf{r}_{\mathrm{A}}$ correctly, no information would be leaked to her due to the high uncorrelation of channels.

4) Bob recovers the coset leader $\mathbf{e}_{\mathrm{A}}$ based on the received syndrome $\mathbf{r}_{\mathrm{A}}$. Then it decodes its own key as:

$$\hat{\mathbf{b}}_{\mathrm{B}} = \arg\min_{\mathbf{b}} \|\mathbf{y}_{\mathrm{B}} - (\mathbf{e}_{\mathrm{A}} + \mathbf{bG})\|. \tag{59}$$

3.3 Lake Test

We conducted four lake tests to examine the performance of the secret key generation protocol shown in Fig. 9. In particular, we took the OFDM modems with single transducer as the nodes to represent Alice, Bob and Eve respectively. The bandwidth of the AquaSeNT OFDM modems is $B = 6$ kHz, with the frequency band 14 kHz to 20 kHz, and the number of total subcarriers is $K = 1024$.

Test 1 was the initial test carried out under the Bassetts Bridge of Mansfield Hollow Lake in Connecticut on Aug. 12, 2014. As Fig. 10(a) shows, the length of the bridge was about 17 meters. All three nodes were put near the walls of the bridge ends, where Alice was on the right side of the bridge, while Bob and Eve were on the opposite side, and 2 meters away from each other. They were deployed about 0.8 meter below the surface, with the water depth of 2 to 3 meters. Being close to the bridge, the nodes were deployed without using a boat. The transmission power of Alice and Bob was set to be -25 dB, where 0 dB refers to the maximum transmission power of 25 Watts allowed by the modem.

After examining the outputs from Test 1, three follow-on tests were carried out in the open water at the Mansfield Hollow Lake on Oct. 3, 2014, as shown in Fig. 10(b), where a boat was used for node deployment. Bob was anchored at a fixed position. In

test 2, Alice was 48 meters away from Bob. In test 3, Alice was apart from Bob with 93 meters. In both tests 2 and 3, Eve was not anchored and floated away with the water flow, and its position was not tracked. In test 4, the distance between Alice and Bob was 179 meters, and Eve was anchored 41 meters away from Bob. In these three tests, Alice and Bob were deployed about 1.5 meters below the water with the transmission power to be -20 dB, and Eve was placed about 1 meter below the water.

(a) Test 1 (b) Tests 2-4

Figure 10: Test locations in the Mansfield Hollow Lake, Connecticut, USA

In test 1, Alice sent the packet number and the probing OFDM blocks every 10 seconds. In tests 2-4, they exchanged packets every 15 seconds. Note that a typical underwater acoustic channel has a coherence time on the order one to several seconds. Once Bob received the probing signal, he replied immediately with the same probing signal, followed by another message to denote the corresponding packet number. Eve listened passively without any interference. In these tests, the syndrome transmission was not carried out, and off-line processing was conducted on the collected data sets. Due to some synchronization and decoding failure, the probing signals with a correct packet number at Alice, Bob and Eve would be used for key generation. In total, we

collected 92 data sets for test 1, 100 sets for test 2, 64 sets for test 3, and 98 sets for test 4.

We use the following metrics to evaluate the performance of the key generation protocol in lake tests.

Bit Match Rate (BitMR): It is defined as the ratio of the number of matched bits to the total number of extracted bits between two parties. The BitMR between Alice and Bob demonstrates the reliability and efficiency for key generation, and the best case is BitMR $= 100\%$. The BitMR between Alice and Eve shows the leaked information. When BitMR $= 50\%$, the best strategy for Eve to crack the key is by random guess.

Burst Match Rate (BurstMR): The BurstMR is the match rate of bursts, by comparing the secret bits extracted from the 64 subcarrier measurements of each burst.

Randomness: The randomness reveals the distribution pattern of bit streams. The standard NIST statistical Test Suite [6] will be used for the randomness measurement of the keys.

3.3.1 Why Amplitudes of CFR?

The amplitude and phase information of channel frequency response (CFR) has been used for key generation in ground wireless communications, respectively [67, 122]. The real part and imaginary part of CFR are also explored and tested for key generation [120]. However, the reciprocity of UWA channel is seldom investigated. Due to the time-varying property, the random sources used in wireless communication may not be applied to that in UWA channels. Assume that impulse responses of the

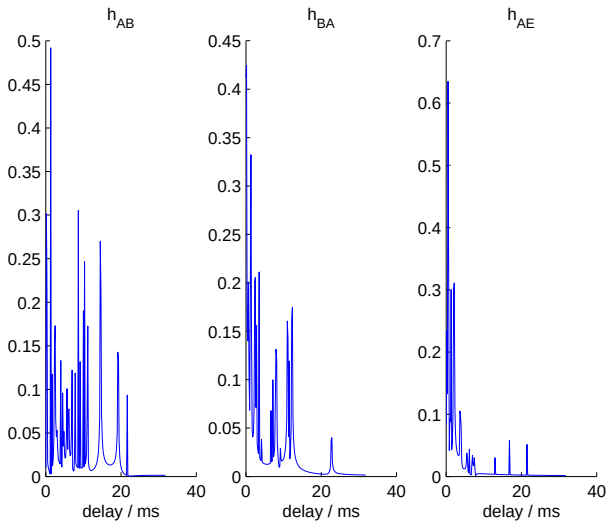
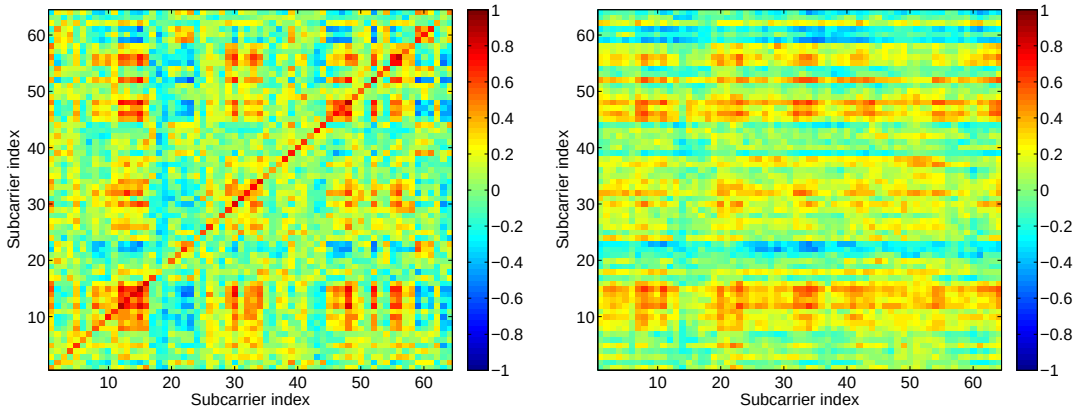


Figure 11: One example plot on the amplitude of the channel impulse responses, lake test 3

legitimate channels measured at Alice and Bob are identical. However, the data acquisition has some delays due to the imperfect synchronization of OFDM modems. A time delay introduces phase rotation in the frequency domain. It is hard to correct the difference of the time delays at two distributed nodes, unless for example the estimates of the channel impulse response could be collected by a central processing unit for time alignment. As a result, the correlation between the CFRs of the mutual channels is very low. It could be worse in half-duplex communication systems by considering the time-varying UWA channels and the channel estimation errors. On the other hand, the amplitude correlation is not affected by the time delay, which could provide more robust performance. Next we verify the reciprocity of the collected UWA channel estimates by the correlation coefficients between CFR amplitudes.

Fig. 12 shows the cross correlation results of the amplitudes of CFR from lake test 3. Due to the limited space, the correlation between real or imaginary parts is not



(a) $(\mathbf{H}_{\mathrm{AB}}, \mathbf{H}_{\mathrm{BA}})$, $\varrho = 0.62$ (b) $(\mathbf{H}_{\mathrm{AB}}, \mathbf{H}_{\mathrm{AE}})$, $\varrho = 0.19$

Figure 12: Cross correlation of CFR amplitudes at 64 equal-spaced subcarriers, lake test 3

shown. If the amplitudes of the CFR are used to compute the correlation coefficients, from Fig. 12(a) we can see that the diagonal is rather clear, and the average correlation coefficient ϱ between legitimate channels are 0.62. Meanwhile, Fig. 12(b) shows that the average correlation coefficient ϱ of the amplitudes of CFR between legitimate channel and eavesdropped channel is about 0.19. Since the correlation coefficients between the legitimate users are larger than that between legitimate user and eavesdropper, we expect secret keys could be extracted from the amplitudes of CFR.

3.3.2 Channel Quantization

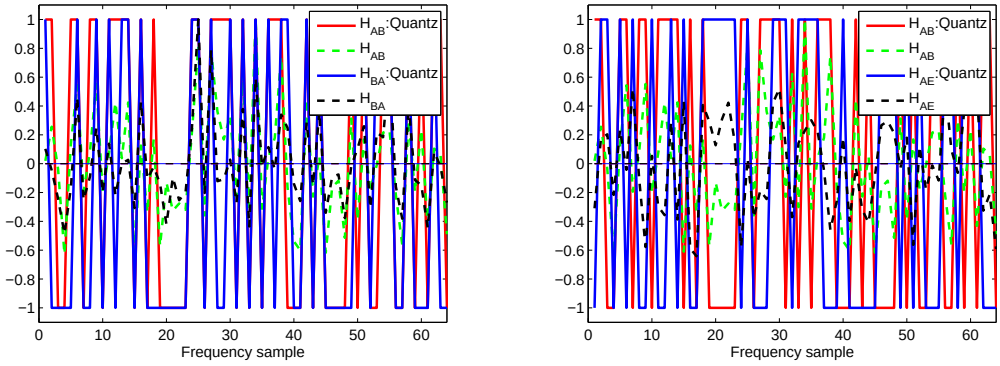
The channels between Alice and Bob $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$, and the channel from Alice to Eve $\mathbf{H}_{\mathrm{AE}}$, are used for key extraction. Although the matrices $\mathbf{H}_{\mathrm{AB}}$, $\mathbf{H}_{\mathrm{BA}}$, and $\mathbf{H}_{\mathrm{AE}}$ have 1024 diagonal entries corresponding to 1024 subcarriers, we select $M = 64$ equal-spaced subcarriers for key generation. The channel frequency amplitudes in Fig. 13

and Fig. 14 are scaled and shifted with the mean to be 0, and range from -1 to 1. Due to the space limitation, only the 1-bit quantization results of test 2 and test 4 are shown.

Fig. 13(a) and 14(a) show the quantization results of the mutual channel in the frequency domain between Alice and Bob for one realization of the two test scenarios. For the scaled estimated channel in the frequency domain, we can see that they are not the same, but with some fluctuations. The motion of medium and buoys, and the imperfection of the modems also impose the asymmetry on the frequency measurements. Define the hamming distance as the number of different bits between two sequences. The Hamming distance shown in Fig. 13(a) is much larger than that in Fig. 14(a), since the water depth was rather small, only about 2 meters, and there were lots of tall water plant at the places where Alice and Bob were deployed. The difference between the quantized $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$ is not as obvious as the unquantized estimates. Part of differences are eliminated by quantization. The differences of quantized values only exist when one channel measurement above the threshold while the other below. Fig. 13(b) and 14(b) show the quantized results of $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$ in the frequency domain. We can see the huge differences not only lie in the scaled channels, but also in the quantized channels. It verifies the low correlation between the legitimate and eavesdropping channels, and implies the feasibility of secret key extraction.

3.3.3 Statistical Property of Quantized Channels

The underwater acoustic channel is time-varying. Figs. 15(a) and 16(a) show the histogram of Hamming distances between quantized $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$, $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$

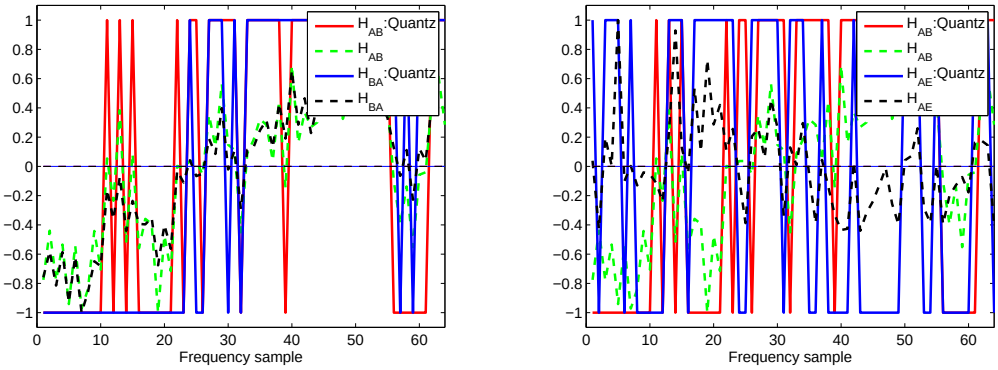


(a) Test 2 (48 m): $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$

(b) Test 2 (48 m): $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$

Figure 13: Scaled channel amplitudes and the corresponding quantized values in the frequency domain of lake test 2, 1-bit quantization. The dashed line represents the normalized channel. The solid line represents the quantized channel.

for test 2 and test 4, when 1-bit quantization is adopted. We see that the Hamming distances between $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$ overlap with the distances between $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$ for test 2. And the distances between $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$ are below 20 for test 4, while the Hamming distances between $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$ are larger than 20 for test 4. Figs. 15(b) and 16(b) show the cumulative probability of Hamming distances for the corresponding channels. It is clear to see the Hamming distances associated with legitimate and eavesdropping channels for test 4 can be separated, and the Hamming distances related to Alice and Bob are smaller than that related to Eve, which verifies the mutual channels have higher correlation, and indicates the possibility to extract secret keys from the channel frequency response between $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$. While for quantized $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$, the mean values increase to about 30 with the standard deviation to be about 4.7, which indicates the lack of correlation between the quantized $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$.



(a) Test 4 (179 m): $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$

(b) Test 4 (179 m): $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$

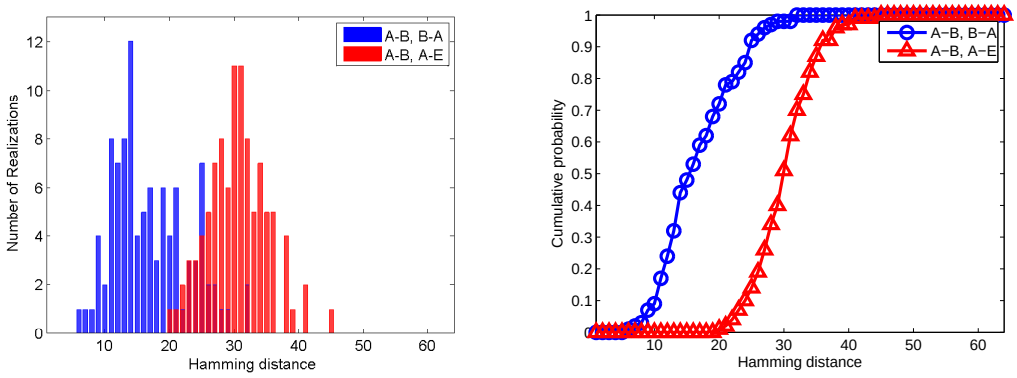
Figure 14: Scaled channel amplitudes and the corresponding quantized values in the frequency domain of lake test 4, 1-bit quantization. The dashed line represents the normalized channel. The solid line represents the quantized channel.

3.3.4 Secret Bits Per Burst

The number of secret bits per burst is determined by the BCH code and the quantization level used in the key generation protocol. The number of secret bits extracted from the BCH code equals to the number of information bits. Since the error correction capability of BCH(n, m) code is discrete, only limited options are available. For each round of information exchange, the number of secret bits can be expressed as

$$r = \lfloor 64/n \rfloor \times m \times q \tag{60}$$

where q is the number of quantized bits per subcarrier, and $q \in \{1, 2\}$. The BCH codes used in this chapter is shown as Fig. 17. The number of secret key bits ranges from are 1 to 56 per burst.



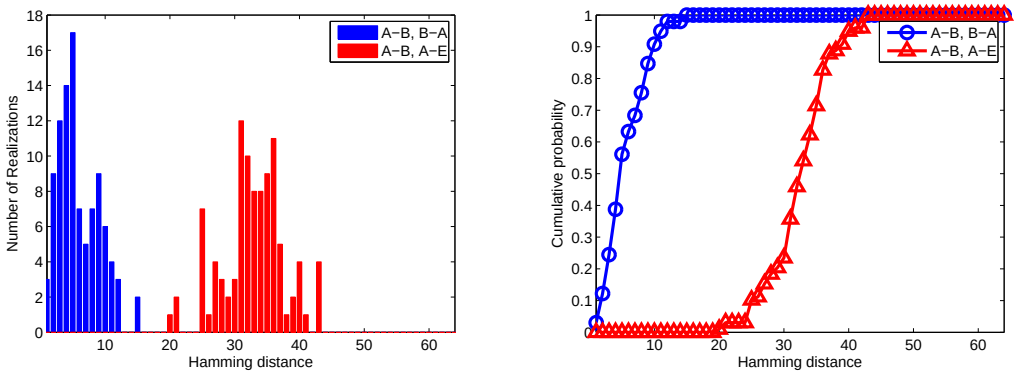
(a) The histogram (b) The cumulative probability

Figure 15: Test 2 (48 m). 1-bit quantization. The Hamming distances between $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$ have mean 17.2, standard deviation 6.2. The Hamming distances between $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$ have mean 30.5, standard deviation 4.6.

3.3.5 Performance Evaluation

Two quantization types are considered for performance comparison. They are listed as: (i) 1-bit quantization; (ii) 2-bit quantization. We take the results of test 3 as an example to show the impact of quantization. From Fig. 18 we can see that when 64 quantized bits are used for secret key extraction each time, 1-bit quantization provides higher BurstMR and BitMR than 2-bit quantization, since 1-bit quantization has better error tolerance than 2-bit quantization but with the price of smaller key generation rate. The BitMR between legitimate user and eavesdropper stays around 0.5 for the two quantization methods, which is a great enlightenment for key generation.

Remark 3. From Fig. 18(a) we can see that when the amplitude of CFR is used for key generation and 22 secret bits are extracted from 64 quantized bits, the corresponding BurstMR is larger than that when 20 secret bits are extracted. It is consistent



(a) The histogram (b) The cumulative probability

Figure 16: Test 4 (179 m). 1-bit quantization. The Hamming distances between $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BA}}$ have mean 5.9, standard deviation 3.1. The Hamming distances between $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{AE}}$ have mean 32.8, standard deviation 4.8.

with the different error correction capability where the corresponding BCH codes are BCH(31,11) and BCH(15,5).

Fig. 19 shows the performance of all the 4 lake tests under the 2-bit quantization. We can see the BurstMR between legitimate users in test 4 are almost 100% even when the key rate is up to 12 bits per 64 quantized bits, while it falls to 40% when the key rate is 28. The BitMR is quite close to 95% even when the key rate is 28, which indicates only small portion of key bits are mismatched in test 4. The BurstMR between the legitimates and Eve drops from 30% to zero quickly, and the corresponding BitMR are around 50%, which implies that Eve can eavesdrop the secret key hardly. For tests 1-3, the BurstMRs drop from around 95% to around 10% quickly as the key rate increases to 20. The BitMRs fall from around 95% to around 75% as the key rate rises to 28. It indicates the importance to select a proper BCH code for key extraction, since

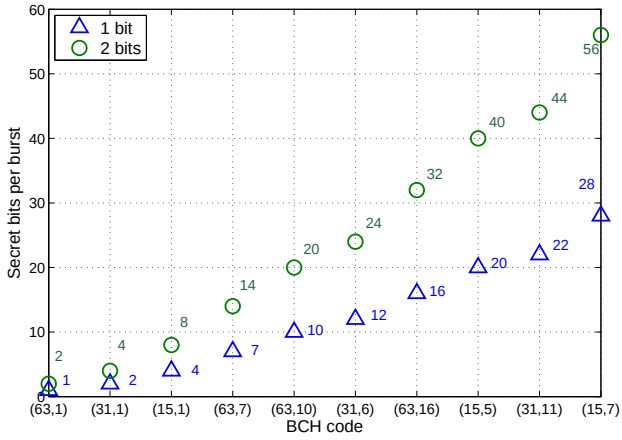
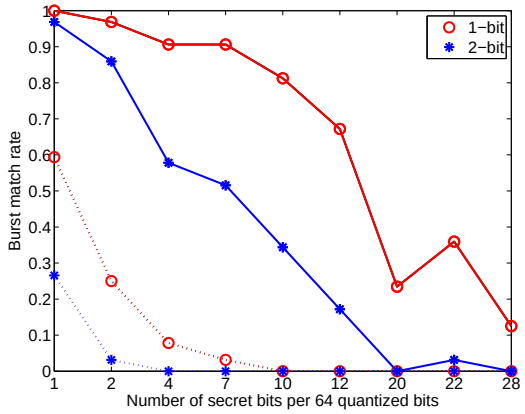


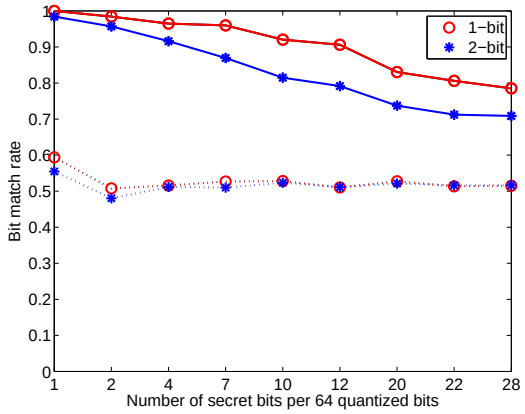
Figure 17: The number of secret key bits, under multi-bit quantization of 64-frequency samples per information exchange

the location of nodes and the environments have a great impact on the BurstMR and BitMR.

Remark 4. From Fig. 19, we can see that tests 1 and 4 have better results than tests 2 and 3. The intuitive explanation is as follows. Since Alice and Bob in test 4 were furthest away from each other in the four tests, only the strong paths could be kept at the receiver side, and the channel would have fewer dominant taps which could be highly correlated. In tests 2 and 3, Alice and Bob were placed much closer compared to test 4. Due to the motion of medium and buoys, and the soft bottom of the lake, more parts of the channel taps might be of low correlation. Test 1 was done in a different geometry and reflection environment. Due to the short distance and the solid bottom and pier reflections, the line-of-sight path and a portion of the reflection paths are quite stable.



(a) Burst match rate

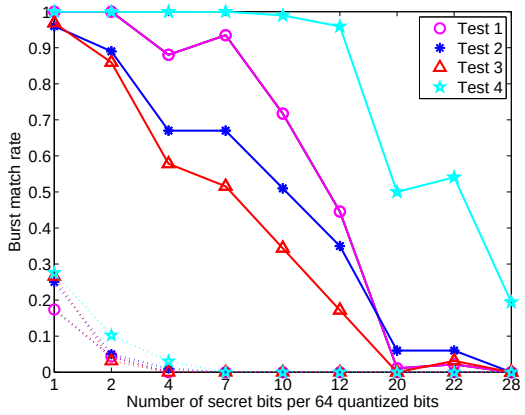


(b) Bit match rate

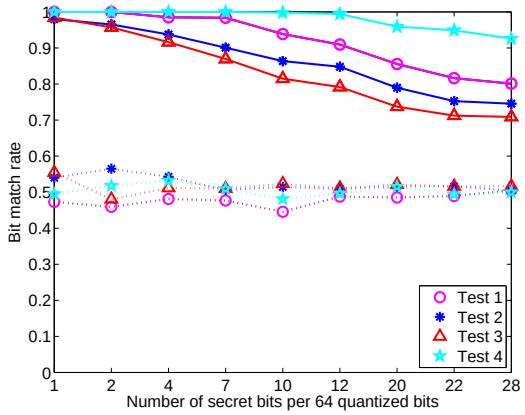
Figure 18: Performance under different quantization methods, lake test 3. Solid lines for $(\mathbf{H}_{\mathrm{AB}},\ \mathbf{H}_{\mathrm{BA}})$; Dotted lines for $(\mathbf{H}_{\mathrm{AB}},\ \mathbf{H}_{\mathrm{AE}})$

3.3.6 Randomness Test

The randomness is a vital metric for the secrecy of keys. The NIST statistical Test Suite provided in [6] is used to test the randomness of keys generated after information reconciliation and privacy amplification. (Note that on-line entropy estimation with the NIST test suite is possible, see e.g., [132], which is out of the scope of this chapter.) If the p-value for a test is greater than 0.01, the generated keys pass the randomness test. In this subsection, we generate keys by using the BCH(15,5) code for the randomness



(a) Burst match rate



(b) Bit match rate

Figure 19: Performance under 2-bit quantization, lake tests 1-4. Solid lines for $(\mathbf{H}_{\mathrm{AB}},\ \mathbf{H}_{\mathrm{BA}})$; Dotted lines for $(\mathbf{H}_{\mathrm{AB}},\ \mathbf{H}_{\mathrm{AE}})$

test. The collected data are limited; e.g., with the BCH(15,5) code, we have $\lceil 64/15 \rfloor \times 5 \times 2 \times 100 = 4000$ bits extracted from test 2. Note that the whole NIST suite provides 15 tests. Some of the tests require a much longer bit sequence to perform a valid test. Here we only choose 9 tests as shown in Table 1. We adopt the SHA-1 hash function to increase the randomness, and assume all the generated 128-bit keys can pass the key verification. Table 1 lists 9 kinds of test results for all the four lake tests. In all of the tests, we divided each bit sequence into multiple streams. If there's no specific

Table 1: Randomness test results by NIST statistical test SUITE for BCH(15,5)

	Test 1 3680 bits	Test 2 4000 bits	Test 3 2560 bits	Test 4 3920 bits
Frequency	0.276	0.534	0.534	0.350
Block Frequency (block size = 128)	0.350	0.122	0.213	0.534
FFT	0.122	0.350	0.350	0.534
Approximate Entropy (block size = 2)	0.350	0.122	0.066	0.067
Cumsum-Forward	0.213	0.911	0.122	0.213
Cumsum-Reverse	0.534	0.991	0.534	0.911
Serial (block size = 5)	0.213 0.911	0.534 0.740	0.911 0.740	0.740 0.34
Long Runs of Ones (block size = 8)	0.162	0.067	0.276	0.862
Runs	<0.01	0.279	0.834	0.232

requirement, 10 data streams are used. If there is a recommend value (minimum or maximum) on the block size, the recommended value is used, which leads to more than 10 data streams. The p-value shown in the table is the aggregated result from the p-values of the available streams. We can see most of the p-values are larger than 0.01, indicating that the generated keys pass the randomness test.

3.4 Protocol Improvement

The lake test results shown in Section 3.3 indicate that when Alice and Bob transmit the probing signal directly, the BurstMR and BitMR are quite low when the correlation of mutual channels is low and a high key rate is desired. The level crossing scheme proposed in [78, 128] made the confirmation of key agreement by exploiting the authentication code generated from the secret message. The hash values are used to confirm the key agreement in [3, 117, 122]. However, the short length of keys leads the key to be cracked easily by exhaustive computation, and longer keys result in low

key agreement rate. e.g. when BitMR is 0.95 and the desired key length is 128, the key agreement probability is as low as $0.95^{128} = 1.4 \cdot 10^{-3}$. So the aforementioned key verification methods fall short of direct practical use.

The improved secret key generation protocol utilizing adaptive pilots to probe the channels and sliced blocks for key verification is shown in Fig. 20. The procedure is similar with the protocol using fixed pilots shown in Fig. 9, but with some differences:

1) In the channel probing phase, instead of replying the known probing signal, Bob forwards a weighted probing signal and the decoded packet number to Alice.

2) In the channel estimation phase, Alice estimates the virtual channel between her and Bob in the frequency domain, rather than the direct channel between them.

3) Step 1) and step 2) will repeat N times, until the desired length of secret bits are obtained. Then the secret bits will be divided into multiple blocks of the same size. Bob generates the hash value of each block, and feeds back the first half of the hash value to Alice in the public channel for key confirmation. Alice compares the received hash values to the bits she generates under the same rule.

4) Alice checks the match of the feedback bits to verify the agreement of keys, and then marks the success and failure of each check. Then Alice sends back the indexes of the matched blocks and the hash values of the overall key bits. If the hash values are the same as that generated by Bob, a key acknowledgement signal will be transmitted to Alice through public channel.

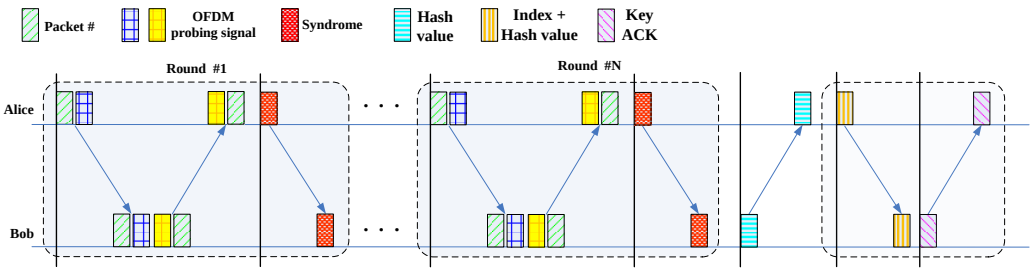


Figure 20: Secret key generation protocol using adaptive probing signal and sliced blocks

3.4.1 Adaptively Weighted Probing Signalling

Suppose that Alice transmits a probing signal $\mathbf{s}_{\mathrm{A}}$ to Bob. After Bob receives the probing signal, he estimates the channel from Alice to Bob as $\hat{\mathbf{H}}_{\mathrm{AB}}$. Instead of transmitting the fixed probing signal $\mathbf{s}_{\mathrm{B}}$, Bob weights the probing signal by the conjugate of the estimated channel $\hat{\mathbf{H}}_{\mathrm{AB}}$. The probing signal sent out by Bob has frequency-domain components as

$$\tilde{\mathbf{s}}_{\mathrm{B}} = \hat{\mathbf{H}}_{\mathrm{AB}}^{*} \mathbf{s}_{\mathrm{B}}. \tag{61}$$

The phase conjugation operation in (61) is motivated by the phase conjugation techniques (also known as time reversal) used for temporal focusing of underwater acoustic channels; see e.g., [36, 126]. Since the channel is changing from round to round, the adaptively generated probing signals would be different at different rounds. Alice and Eve would observe

$$\tilde{\mathbf{z}}_{\mathrm{A}} = \mathbf{H}_{\mathrm{BA}} \tilde{\mathbf{s}}_{\mathrm{B}} + \boldsymbol{\eta}_{\mathrm{E}} = \left(\mathbf{H}_{\mathrm{BA}} \hat{\mathbf{H}}_{\mathrm{AB}}^{*} \right) \mathbf{s}_{\mathrm{B}} + \boldsymbol{\eta}_{\mathrm{E}}, \tag{62}$$

$$\tilde{\mathbf{z}}'_{\mathrm{E}} = \mathbf{H}_{\mathrm{BE}} \tilde{\mathbf{s}}_{\mathrm{B}} + \boldsymbol{\eta}'_{\mathrm{E}} = \left(\mathbf{H}_{\mathrm{BE}} \hat{\mathbf{H}}_{\mathrm{AB}}^{*} \right) \mathbf{s}_{\mathrm{B}} + \boldsymbol{\eta}'_{\mathrm{E}}. \tag{63}$$

Bob can get the estimated channel $\hat{\mathbf{H}}_{\mathrm{AB}}$ from the probing signals and observations. Since Alice only has the shared pilot information, she can estimate the weighted channel $\hat{\mathbf{H}}^{*}_{\mathrm{AB}}\mathbf{H}_{\mathrm{BA}}$ through channel estimation where the Least Squares channel estimator is used [52]. The estimated weighted channel from Bob to Alice is here expressed as $\breve{\mathbf{H}}_{\mathrm{BA}}$ for clarity.

As discussed in Section 3.3.1 that only the amplitude of CFR will be used for key generation in UWA channels, and the phase information will be ignored. If the channel is perfectly reciprocal, then $|\hat{\mathbf{H}}_{\mathrm{BA}}|$ at Alice is identical to $|\hat{\mathbf{H}}^{*}_{\mathrm{AB}}|$ at Bob. If the mutual channels are not reciprocal but correlated, the virtual CFR on the kth subcarrier between Bob and Alice, as estimated at Alice, is

$$|\tilde{H}_{\mathrm{BA}}[k]| = \sqrt{|\breve{H}_{\mathrm{BA}}[k]|} \approx \sqrt{|\hat{H}^{*}_{\mathrm{AB}}[k]||\hat{H}_{\mathrm{BA}}[k]|}, \tag{64}$$

If $|\hat{H}_{\mathrm{BA}}[k]|$ at Alice is smaller than $|\hat{H}^{*}_{\mathrm{AB}}[k]|$ at Bob, due to the square root function of the multiply of the two estimated channels, we would have

$$|\hat{H}_{\mathrm{BA}}[k]| < |\tilde{H}_{\mathrm{BA}}[k]| < |\hat{H}^{*}_{\mathrm{AB}}[k]|, \tag{65}$$

which means $|\tilde{H}_{\mathrm{BA}}[k]|$ at Alice is closer to $|\hat{H}^{*}_{\mathrm{AB}}[k]|$ than $|\hat{H}_{\mathrm{BA}}[k]|$. On the other hand, if $|\hat{H}_{\mathrm{BA}}[k]|$ at Alice is greater than $|\hat{H}^{*}_{\mathrm{AB}}[k]|$ at Bob, we have

$$|\hat{H}^{*}_{\mathrm{AB}}[k]| < |\tilde{H}_{\mathrm{BA}}[k]| < |\hat{H}_{\mathrm{BA}}[k]|, \tag{66}$$

and we have the same conclusion that $|\tilde{H}_{\mathrm{BA}}[k]|$ at Alice is closer to $|\hat{H}^{*}_{\mathrm{AB}}[k]|$. So we expect the correlation between $|\hat{H}_{\mathrm{AB}}[k]|$ and $|\tilde{H}_{\mathrm{BA}}[k]|$ would increase.

Note that Eve has the option of generating the keys from $\hat{\mathbf{H}}_{\mathrm{AE}}$ or from $\hat{\mathbf{H}}_{\mathrm{BE}}$. The correlation of CFR amplitudes between $\hat{\mathbf{H}}_{\mathrm{AB}}$ and $\hat{\mathbf{H}}_{\mathrm{AE}}$ is not affected by adaptive probing, but the correlation of CFR amplitudes between $\hat{\mathbf{H}}_{\mathrm{AB}}$ and $\hat{\mathbf{H}}_{\mathrm{BE}}$ might increase when Bob's probing signal incorporates part of the channel information from $\hat{\mathbf{H}}_{\mathrm{AB}}$. The advantage and disadvantage of adaptive probing will be evaluated in Section 3.5 where Eve generates the keys with $\hat{\mathbf{H}}_{\mathrm{BE}}$.

3.4.2 Block-Sliced Key Verification

Although the error correction code BCH(n, m) can reduce the bit mismatch rate, the legitimate users still need to check the agreement of keys at both parties. Otherwise, the bit stream cannot be used as secret keys. In this chapter, we introduce the block-sliced key verification module to handle the channel dynamics, which uses part of hash values of the extracted information code words to verify the consistency of keys.

After N rounds of mutual communication, Alice and Bob collect mN consecutive secret bits. The mN bits will be sliced into N_{bl} blocks of size N_{s}, where

$$N_{\mathrm{bl}} = \left\lfloor \frac{mN}{N_{\mathrm{s}}} \right\rfloor . \tag{67}$$

For each block, Bob computes the corresponding 128-bit hash value by using the SHA-1 hash function, and the first N_{s} bits of the hash value will be kept as effective bits since the last $128 - N_{\mathrm{s}}$ bits are redundant as keys. The first N_{f} bits of the effective bits will be fed back to Alice for key agreement verification. Alice generates the hash value of each block with the same criteria as Bob. Then she compares the first N_{f}-bit hash value to her received hash value block by block. If they are matched, Alice can claim

she and Bob share the same block information, and the indexes of the matched blocks will be recorded. Meanwhile, the remaining $N_{\mathrm{s}} - N_{\mathrm{f}}$ bits will be kept as the keys.

If all the N_{s}-bit long sequences are of equal probability, the block mismatch probability between legitimate users is $1 - \frac{1}{2^{N_{\mathrm{s}}-N_{\mathrm{f}}}}$. Obviously, the longer N_{f} is, the lower the false match rate is, but the key generation rate decreases too.

To make sure that the key is hard to crack computationally, the desired length of the final key N_{k} should be long enough. Alice cascades the short keys from the blocks that pass the match check. Once the accumulative key length is larger than N_{k}, Alice will truncate the first N_{k} bits, and send both the indexes of the corresponding matched blocks and the hash value of the final key to Bob. Bob concatenates the secret keys from the matched blocks, and derive the corresponding hash values. Then he compares the hash values from himself to that from Alice. At last Bob will send a key acknowledgement to Alice, to inform her whether the final keys passed the check or not. While Eve would extract keys based on the overheard indexes of matched blocks, regardless of the match of the feedback bits to her observation.

Remark 5. Consider that the secret bits after information reconciliation are matched with a high probability, and similar bit sequences will result in very different hash values, so we only use part of the hash value for the block match check at first. Since hash function would have collisions, we would like to feedback proper amount of bits to cut down the collisions and reduce the key mismatch rate. Finally we take another round of hash function to verify the agreement of the N_{k}-bit key.

3.5 Numerical Simulations

The parameters of the ZP-OFDM communication system considered for simulation are as follows: center frequency $f_{\mathrm{c}} = 13$ kHz, bandwidth $B = 9.77$ kHz, symbol duration $T = 104.86$ ms, guard interval $T_{\mathrm{g}} = 24.6$ ms. The ZP-OFDM system has $K = 1024$ subcarriers in total. The simulated UWA channel has 15 discrete paths. The inter-arrival time of paths is exponentially distributed with mean of 1 ms, resulting a 15-ms channel delay spread on average. The amplitude of each path follows Rayleigh distribution with an exponential power decay profile, and the attenuation difference between the beginning and end of the guard time is 20 dB [52]. The UWA channels are assumed to follow block fading, and the Doppler effect is not considered. A total of 1000 Monte Carlo runs are carried out for key generation.

Assume that the path delays of Alice and Bob are the same. Define $h_{\mathrm{A},l}$ and $h_{\mathrm{B},l}$ as the lth channel coefficient of Alice and Bob, respectively. Assume that $[h_{\mathrm{A},l}\ h_{\mathrm{B},l}]^T$ follows the correlated complex Gaussian distribution

$$\begin{bmatrix} h_{\mathrm{A},l} \\ h_{\mathrm{B},l} \end{bmatrix} \sim \mathcal{CN}\left(\begin{bmatrix} 0 \\ 0 \end{bmatrix},\ \sigma_h^2 \begin{bmatrix} 1 & \rho \\ \rho & 1 \end{bmatrix} \right), \tag{68}$$

where ρ is the correlation coefficient. Then the correlated lth channel coefficient can be modeled as

$$h_{\mathrm{B},l} = \rho h_{\mathrm{A},l} + \sqrt{1-\rho^2}\zeta_l, \tag{69}$$

where $h_{\mathrm{A},l}$ and ζ_l follow independent complex Gaussian distributed with $\mathcal{CN}(0, \sigma_h^2)$. Note that Fig. 12(a) reports an average correlation between the CFR amplitudes of

$\varrho = 0.62$. When the correlation of the path amplitudes is $\rho = 0$, the simulated CFR amplitudes $|H_{\mathrm{AB}}[k]|$ and $|H_{\mathrm{BA}}[k]|$ have an average correlation of $\varrho = 0.63$, due to the shared channel delay structure. When $\rho = 0.5$, the average correlation of the CFR amplitudes increases to $\varrho = 0.69$.

The channel coefficient of Eve is assumed to have the same but independent distribution as Alice and Bob, and the path delay of Eve follows the same distribution as Alice and Bob, but independent. The average correlation between the CFR amplitudes $|H_{\mathrm{AB}}[k]|$ and $|H_{\mathrm{AE}}[k]|$ (or between $|H_{\mathrm{AB}}[k]|$ and $|H_{\mathrm{BE}}[k]|$ when fixed pilots are used) is $\varrho = 0.01$.

3.5.1 Metrics

Besides the metrics introduced in Section 3.3, we add one more metric, *average key length*, to evaluate the performance of the proposed protocol with adaptive pilots and block-sliced key verification. The average key length is defined as the key rate agreed between legitimate users per channel probing, which equals the number of matched blocks times the number of secret keys per block, then divided by 1000 (the number of rounds):

$$\overline{L}_1 = N_{\mathrm{blk}}(N_{\mathrm{s}} - N_{\mathrm{f}})/1000. \tag{70}$$

The average key length as in (70) is the common metric that has been used in [67, 86, 122, 127] to show the key generation speed. Compared to the number of secret bits in Section 3.3.4, the average key length as in (70) reflects the number of bits per channel probing after considering the impact of information reconciliation and key verification.

Note that the average key length as in (70) only describes the shared key rate that legitimate users can agree per channel probing, but it does not account for the potential information leakage to Eve. Basically, the secrecy rate is the difference between the mutual information on legitimate channels and the eavesdropping channel [1, 14, 79], and the maximal secrecy rate is the achievable secrecy capacity [141]. Inspired by the definition of the secrecy capacity in [141] and the entropy of the final key in [97], we revise the definition of the average key length, by taking into account the difference of the entropy on the key bits of the legitimate nodes and eavesdropper as follows.

Denote the binary bits at Alice, Bob and Eve as $b_{\rm A}, b_{\rm B}$ and $b_{\rm E}$, respectively. The rate of the secret key bits between legitimate users and eavesdropper can be expressed as[2] [97, 141]:

$$r_{\rm s} = I(b_{\rm A}; b_{\rm B}) - I(b_{\rm A}; b_{\rm E}) = [H(b_{\rm A}) - H(b_{\rm A}|b_{\rm B})] - [H(b_{\rm A}) - H(b_{\rm A}|b_{\rm E})]. \quad (71)$$

Since $b_{\rm A} = b_{\rm B}$ after key verification, (71) can be simplified to

$$r_{\rm s} = H(b_{\rm A}|b_{\rm E}) = -E\{\log p(b_{\rm A}|b_{\rm E})\}. \quad (72)$$

Expanding (72), we have

$$r_{\rm s} = \sum_{i,j=0}^{1} p(b_{\rm A} = i, b_{\rm E} = j) \log \frac{1}{p(b_{\rm A} = i|b_{\rm E} = j)}. \quad (73)$$

The joint probability $p(b_{\rm A} = i, b_{\rm E} = j)$ and conditional probability $p(b_{\rm A} = i|b_{\rm E} = j)$ can be derived from the data for offline analysis. Then the average key length with

[2] In order to achieve the rate of (71), a public communication channel of unlimited capacity is required.

N_{blk} blocks that passed the match check is computed as

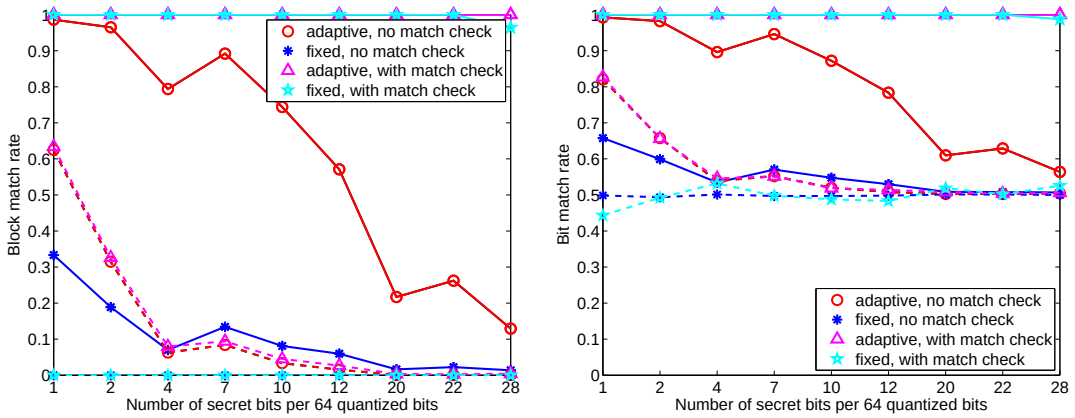
$$\overline{L}_2 = N_{\mathrm{blk}}(N_{\mathrm{s}} - N_{\mathrm{f}})r_{\mathrm{s}}/1000. \tag{74}$$

Since $r_{\mathrm{s}} \in [0, 1]$, one has $\overline{L}_2 \leq \overline{L}_1$, where the equality holds when no information is leaked to Eve.

3.5.2 Performance Evaluation

In the simulation, we set the channel correlation coefficient between Alice and Bob to be $\rho = 0.5$, and the channel correlation coefficient between legitimate users and Eve to be zero. (The case with $\rho = 0$ for the channels between Alice and Bob is also tested and not reported here as the observations are similar.) The signal-to-noise ratio (SNR) of each channel is 20 dB. The 2-bit quantization across subcarriers in frequency domain is taken as an example to show the performance. The block size is set to be $N_{\mathrm{s}} = 28$, and the number of feedback bits is $N_{\mathrm{f}} = 14$. So Alice hashes the 28 secret bits, and feedback 14 bits to Bob for key verification, and the remaining 14 bits may be kept as keys if the match check is passed.

Fig. 21 shows the simulation results of the key generation protocol using fixed or adaptive pilots with/without key verification, respectively. If the key verification process is not carried out, the BlockMR is the match rate of blocks between two parties. If the key verification is adopted, the BlockMR is the ratio of the number of the matched blocks compared to the number of the check-passed blocks, which reflects the correct check rate. We can see that both the BlockMR and BitMR under the protocol using adaptive pilots shows better performance over the protocol using fixed pilots. If key



(a) Block match rate (b) Bit match rate

Figure 21: Simulation result with $\rho = 0.5$, 2-bit quantization, under 20 dB. Solid lines for $(\mathbf{H}_{\mathrm{AB}},\ \mathbf{H}_{\mathrm{BA}})$; Dotted lines for $(\mathbf{H}_{\mathrm{AB}},\ \mathbf{H}_{\mathrm{BE}})$

verification is used, the BlockMR and BitMR between legitimate users can increase to 100%, and the protocol using adaptive pilots is more robust than the protocol using fixed pilots even when 28 secret bits can be extracted per 64 quantized bits, which indicates the effectiveness of the improved key verification approach. If the match check is not carried out, the improvement of BlockMR and BitMR under the protocols using fixed pilots and adaptive pilots decrease gradually as the key rate grows. The protocol using adaptive pilots will leak some information to Eve especially when the key rate is low. However, the leakage (BlockMR and BitMR between legitimate users and Eve) decreases as the key rate increases, which implies that the protocol using adaptive pilots enhances the potential to increase the BlockMR, BitMR and key rate without leaking any information.

Fig. 22 shows the average key length per round under the scheme of fixed and adaptive pilots. For the average key length as defined in (70), we can see that $\overline{L}_1$

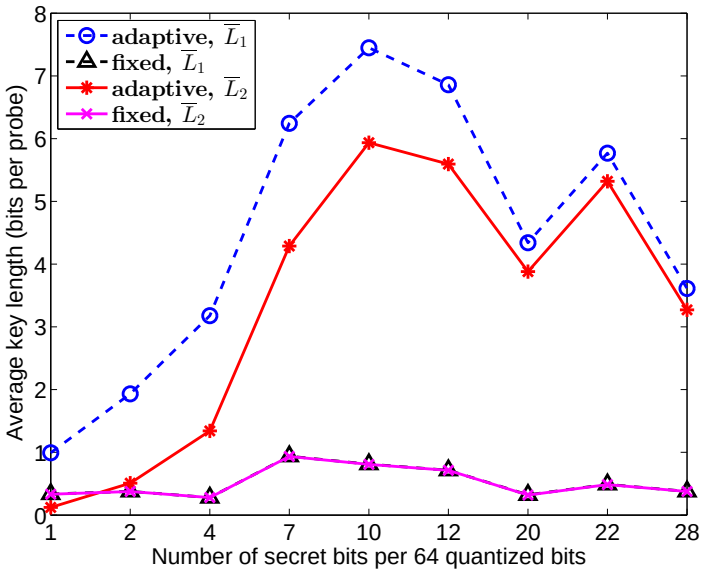


Figure 22: Simulation result of mutual channels $(\mathbf{H}_{\mathrm{AB}},\ \mathbf{H}_{\mathrm{BA}})$, with $\rho = 0.5$, 2-bit quantization, under 20 dB.

using fixed pilots stays around 0.5. The protocol using adaptive pilots provides larger $\overline{L}_1$ than that using fixed pilots, since more blocks can pass the match check in the key verification phase when the weighted probing signalling is used. As more secret bits can be extracted per 64 quantized bits, the average key length increases at the beginning due to a higher amount of matched blocks, and then drops because of the lower error correction ability of BCH codes used and less matched blocks.

For the average key length $\overline{L}_2$ as defined in (74), we can see that when 1 secret bit is extracted per 64 bits, the protocol using adaptive pilots has a smaller average key length than that using fixed pilots, since some of the agreed keys between Alice and Bob are leaked to Eve. However, as more secret bits can be generated per 64 bits which means less information are leaked to Eve, the average key length increases to 6

Table 2: Randomness test results by NIST statistical test SUITE when $\rho = 0.5$, $N_{\mathrm{s}} = 28$, $N_{\mathrm{f}} = 14$, 2-bit quantization, and SNR = 20 dB

	BCH(15,1) 3178 bits	BCH(31,6) 3612 bits	BCH(15,7) 6860 bits
Frequency	0.534	0.637	0.437
Block Frequency (block size = 128)	0.351	0.213	0.350
FFT	0.534	0.067	0.911
Approximate Entropy (block size = 2)	0.739	0.350	0.163
Cumsum-Forward	0.534	0.213	0.350
Cumsum-Reverse	0.534	0.534	0.911
Serial (block size = 5)	0.911 0.740	0.350 0.350	0.122 0.534
Long Runs of Ones (block size = 8)	0.122	0.025	0.063
Runs	0.122	0.437	0.115

bits which indicates the advantage of the key generation protocol using adaptive pilots, while the average key length with fixed pilots stays around 0.5 bit.

For the protocol with fixed pilots, we can see the average key length under different definitions are nearly the same, since the eavesdropping channel is uncorrelated to the legitimate channel. For the protocol with adaptive pilots, $\overline{L}_2$ is slightly smaller than $\overline{L}_1$, since the weighted forwarding signalling would leak some information to Eve.

3.5.3 Randomness Test

We use the NIST statistical Test Suite to test the randomness of keys which are generated by using three different kinds of BCH codes under the protocol using adaptive pilots. Table 2 shows the corresponding p-values of the nine tests. We can see all the p-values are larger than 0.01, indicating that the keys pass the randomness test successfully.

3.6 Conclusion

In this chapter, we first presented a secret key generation approach which uses fixed pilots to probe the UWA channel. The multi-bit quantization is carried out based on the statistical information across subcarriers, and the channel frequency responses of UWA channels are used for key extraction. The lake test results verified the reciprocity and randomness of the amplitudes of UWA channel frequency responses, and demonstrated that secret key generation is achievable by selecting proper error correction codes. However, the low correlation between mutual channels showed in the lake tests hinders a higher bit match rate when more secret bits are desired. To improve the bit match rate and make the secret key generation approach more practical, we proposed an improved key generation approach, which uses weighted forward probing signalling to improve the correlation of channel frequency response, and adopts the sliced-block key verification approach to deal with the channel dynamics. Simulation results show that our proposed approach has better bit match rate, and longer key length when less information is leaked during the reconciliation phase.

Chapter 4

A Half-Duplex Self-Protection Jamming Approach for Improving Secrecy of Block Transmissions in Underwater Acoustic Channels

4.1 Introduction

Security is one critical issue in underwater acoustic (UWA) communications [33]. Due to the broadcast nature of the underwater acoustic channels, the transmitted packet can be heard by legitimate destinations as well as by eavesdroppers or unauthorized nodes [54]. In addition to encrypting the information by the secret key generated from mutual channels, improving the physical layer security by jamming is another important way to make sure that the correct information can be delivered to the legitimate destination while keeping the message protected from the eavesdropper.

In the radio domain, a lot of approaches have been proposed to enhance the physical layer security, aiming to achieve a large secrecy capacity or secrecy rate. One

interesting approach is to use cooperative relays as helpers to disrupt the eavesdropper. The work in [73] considered a Gaussian wiretap channel model with a single-antenna source, destination, and eavesdropper and proposed a nulling scheme to maximize the system secrecy rate while creating no interference to the destination. The work in [34] considered another scenario in which the relay was equipped with multiple antennas and proposed a system design for determining the antenna weights and transmit power of the source and relay, so that the system secrecy rate was maximized subject to a total transmit power constraint or the transmit power was minimized subject to a secrecy rate constraint. The problem can be extended to the condition that the energy is harvested from nature [21, 45]. Further, the work in [35] addressed secure communications considering three cooperative schemes: decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ), and aimed at the determination of relay weights and the allocation of transmit power.

Recently, using a full-duplex receiver as the jamming source without help from relays has received some attention. In [63], the approach that the full-duplex legitimate receiver could generate artificial noise to jam the eavesdropper was proposed, and the outage secrecy region was used to analyze the secrecy performance from the perspective of geometry. The work in [18] proposed to use both the transmitter and receiver for full duplex beamforming, to improve the throughput and secrecy under the constraint of the guaranteed secrecy and QoS for legitimate users. The joint time and power allocation in full-duplex (FD) wireless-powered communication network

was studied in [57], where the average and peak transmit power were constrained to maximize the weighted sum-rate.

However, the characteristics of underwater acoustic channels, such as large delay spread, limited acoustic link capacity, and multipath effect have differed the underwater acoustic communication significantly from the ground wireless communication [19, 20, 61, 75, 140]. The approaches aforementioned are neither applicable nor effective to protect the underwater communication information. Until now, most work about underwater communication security is done on the network layer and little attention has been paid on the use of jamming signals to improve the physical layer security.

In this chapter, we investigate an underwater acoustic system where Alice is transmitting messages to Bob in presence of Eve [53]. Since typical underwater transceivers are half-duplex, Bob can send jamming signals during the guard intervals between successive blocks it receives from Alice. By making use of the large propagation delay in underwater channels, the interference from the jamming signal will overlap with the information blocks at Eve, thus preventing the protected message from being eavesdropped. The main contributions of this chapter are as follows.

1) We take advantage of the large propagation delay in underwater acoustic channels so that the jamming signal will collide with the message block to make the information from Alice corrupted at Eve's side. In this way, we do not need to specially design the jamming noise that will cancel out at Bob's side while making the biggest interference to Eve.

2) The destination node (Bob) works on a half-duplex scheme. The proposed protocol does not need additional helpers, is easy to implement, and will avoid excess resources.

Clearly the success of the proposed approach utilized the unique properties of underwater acoustic communications: 1) half-duplex transceiver, and 2) large propagation delay. This is along the same lines of recent works in [30, 112, 129]. Specifically, the propagation delay was exploited for interference alignment in underwater acoustic networks in [30], which proposed computationally efficient scheduling protocols for a large throughput improvement. Through transmitter selection and timing control, the signal alignment approach in [112] could increase the communication secrecy in a distributed antenna system. A distributed interference alignment scheduling algorithm, named Shark-IA, was proposed for a multi-hop underwater acoustic network with half-duplex communication systems, which improved the network throughput by exploiting the propagation delays [129].

The organization of the rest of this chapter is as follows: Section 4.2 describes the proposed half-duplex jamming approach. Section 4.3 provides detailed analysis based on cyclic-prefixed orthogonal frequency divided multiplexing (OFDM) transmissions. Simulation results are given in Section 4.4 and conclusions are drawn in Section 4.5.

4.2 The Proposed Half-Duplex Jamming Approach

Consider the basic half-duplex communication system with 3 nodes as Fig. 23 shows. Alice and Bob are two legitimate nodes where Alice sends information to

Bob. Eve overhears the communication between the legitimate nodes passively. To hinder Eve from intercepting the transmitted information, usually extra helpers have to cooperate with Alice, by sending out jamming signals to interfere with the signals sent by Alice. However, if no helpers are available, the system can adopt a self-protection scheme to achieve secure communication [138, 139]. Considering Bob works in a half-duplex mode in underwater acoustic communications, and the guard intervals between successive blocks are typically large, Bob can work as a temporary helper to jam Eve without affecting his own reception of useful signals.

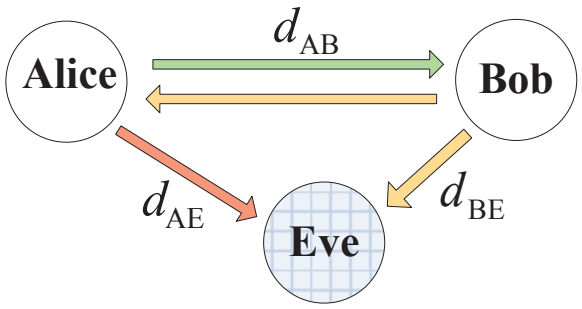


Figure 23: Jamming topology with a half-duplex receiver

4.2.1 Jamming on Cyclic Prefixed Block Transmissions

Cyclic prefixed block transmissions have been extensively studied under both single-carrier underwater communications [47, 113] and multicarrier underwater communications [2, 10, 29, 40, 42, 60, 94].

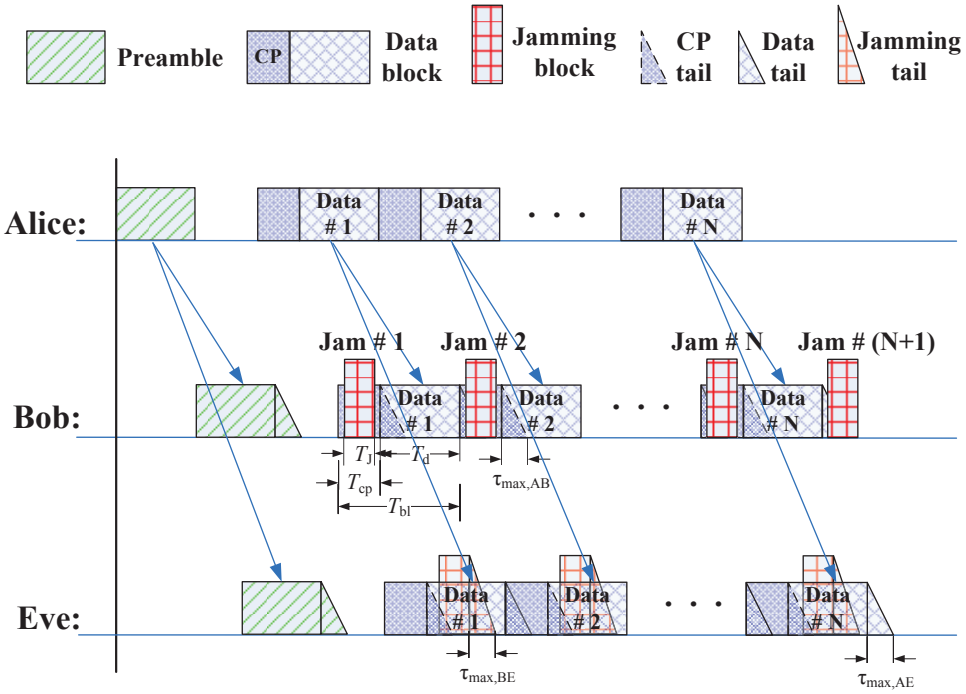
Alice sends out one packet to Bob, where the packet consists of one preamble block and N data blocks. Assume that each block has a duration T_{d}. A cyclic prefix (CP)

of length T_{cp} is inserted between consecutive blocks to avoid possible inter-block interference and to facilitate frequency-domain processing at the receiver. This requires that T_{cp} is larger than the delay spread $\tau_{\mathrm{max,AB}}$ of the underwater acoustic channel $h_{\mathrm{AB}}(t)$ between Alice and Bob.

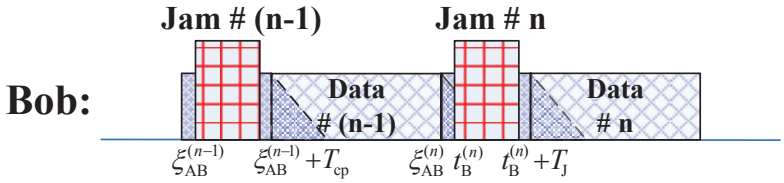
The jamming schedule on block transmission with cyclic prefix of a 3-node communication system is shown in Fig. 24(a). After acquiring the preamble, Bob starts to receive the data part of the packet. Since the CP part of each block does not need to be recorded for data decoding, Bob transmits jamming signal during the CP period by switching the receiver/transmitter mode. If one more jamming block will be transmitted after the last data block is received, there are totally $N + 1$ jamming blocks that could help to protect the communication system.

The basic requirement for the half-duplex jamming schedule is to interfere Eve by the jamming signal from Bob, while taking advantage of the available time $T_{\mathrm{J,max}}$ as much as possible. Suppose that the switch interval between transmitting mode and receiving mode of Bob is negligible, the maximal jamming duration that Bob can occupy is $T_{\mathrm{J,max}} = T_{\mathrm{cp}} - \tau_{\mathrm{max,BB}}$, where $\tau_{\mathrm{max,BB}}$ is the maximum delay spread considering the reverberation effect of the transmission from Bob himself.

The maximal jamming duration that Eve could suffer is $T_{\mathrm{J,max}} + \tau_{\mathrm{max,BE}}$, where $\tau_{\mathrm{max,BE}}$ is the delay spread of the channel $h_{\mathrm{BE}}(t)$ between Bob and Eve. Due to the slow sound propagation speed, the jamming from Bob would not be synchronized at the block level with the original signal from Alice, thus considerably deteriorating the performance at Eve.



(a) Jamming schedule



(b) Time stamp at Bob

Figure 24: Jamming protocol for half-duplex block transmission communication systems with cyclic prefix

4.2.2 Jamming on Zero-Padded Block Transmissions

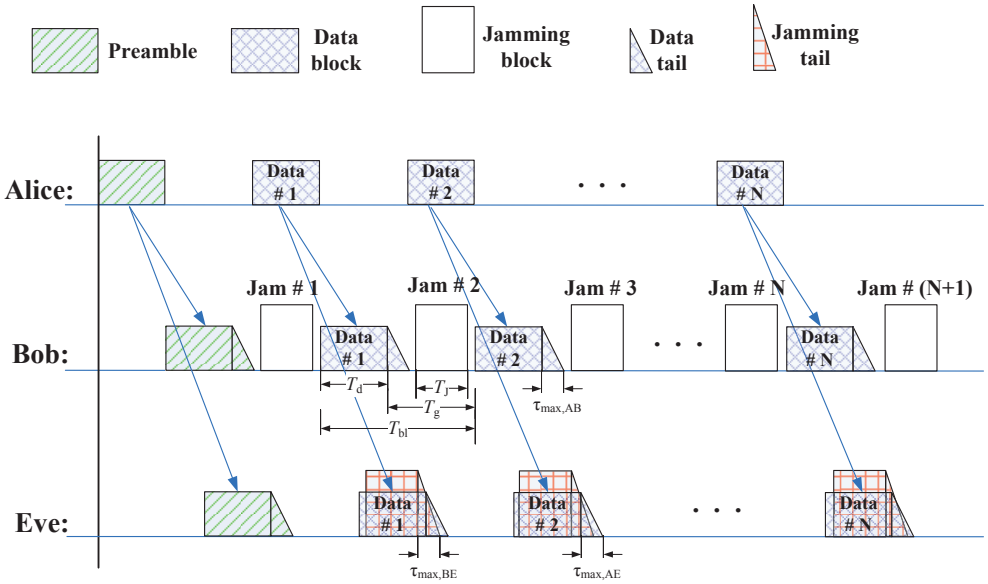
Zero-padded (ZP) block transmission is another popular way of underwater acoustic communications for lower power consumption, such as single-carrier ZP block transmission [133, 134], and multicarrier transmission in the form of ZP-OFDM [11, 71, 72, 105, 106, 110, 115].

Fig. 25(a) shows the jamming schedule on block transmissions with zero padding of a 3-node communication system, which is similar to the communication systems with cyclic prefix. Since the CP part is replaced by zero-padding guard interval of duration $T_{\rm g}$, the corresponding jamming schedule for zero padding communication system is slightly different. The total block duration is $T_{\rm bl} = T_{\rm d} + T_{\rm g}$. Assume the delay spread $\tau_{\rm max,AB}$ of the channel $h_{\rm AB}(t)$ can be estimated from the preamble and the synchronization works perfect. Since the block processing needs to collect samples of duration $T_{\rm d} + \tau_{\rm max,AB}$, the maximal time period for jamming that Bob can occupy is $T_{\rm J,max} = T_{\rm g} - \tau_{\rm max,AB} - \tau_{\rm max,BB}$. If the length of $T_{\rm cp}$ is equal to the length of $T_{\rm g}$, then cyclic prefixed block transmission provides longer time duration for jamming than zero-padded transmission.

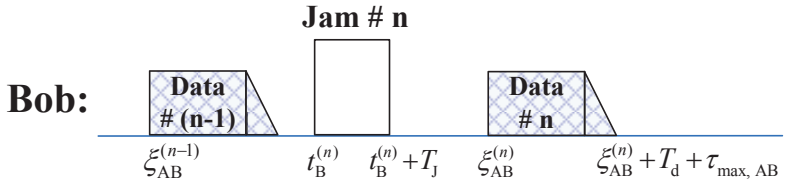
In the rest of the chapter, we explore the half-duplex jamming receiver based on cyclic prefixed OFDM transmissions.

4.2.3 Extension to two-way communications

The main body of this chapter deals with the one way communication from Alice to Bob, where Bob sends out self-protection jamming signals. To further increase the security, a two-way or three-way handshaking protocol can be used to establish the communication between Alice and Bob. After Bob receives a message from Alice, he will reply with an acknowledgment in response to the successful transmission of the information. This is the two-way handshaking process. In three-way handshaking,



(a) Jamming schedule



(b) Time stamp at Bob

Figure 25: Jamming protocol for half-duplex block transmission communication systems with zero padding

finally Alice will send the acknowledgment back to the Bob, to prevent Bob from sending the acknowledgment again if there is a delayed duplicate synchronized message.

Eve will receive information from both Alice and Bob simultaneously. Both Alice and Bob can adopt the self-protection jamming scheme when receiving a message during the handshaking process. This extension is worthy mentioning here, but our following analysis is based on the one-way communication from Alice to Bob.

4.3 Secrecy Rate for CP-OFDM

We now analyze the three-node system assuming that the transmitted data blocks from Alice to Bob are CP-OFDM, and the jamming blocks from Bob to Eve are Gaussian noises with a flat spectrum across the signal band.[1]

4.3.1 CP-OFDM Transmission

The CP-OFDM signal structure for the data blocks is considered as in [77]. Let $T_{\rm d}$ denote the symbol duration, $T_{\rm cp}$ the length of the cyclic prefix. The total CP-OFDM block duration is $T_{\rm bl} = T_{\rm d} + T_{\rm cp}$. Denote B as the bandwidth and K as the total number of used subcarriers. The subcarrier spacing is $\triangle f = 1/T_{\rm d} = B/K$. The mth subcarrier in passband is

$$f_m = f_{\rm c} + \frac{m}{T_{\rm d}}, \quad m = -\frac{K}{2}, \ldots, \frac{K}{2} - 1 \tag{75}$$

where $f_{\rm c}$ is the center frequency. Let $s_{\rm A}[m;n]$ denote the symbol to be transmitted on the mth subcarrier of the nth block. Since one packet consists of N data blocks, the transmitted signal in passband from Alice can be expressed as

$$\tilde{x}_{\rm A}(t) = \sum_{n=1}^{N} \tilde{x}_{\rm A}(t - (n-1)T_{\rm bl}; n),\ t \in [-T_{\rm cp}, NT_{\rm bl} - T_{\rm cp}] \tag{76}$$

where the nth transmitted data block is

$$\tilde{x}_{\rm A}(t;n) = 2{\rm Re}\Big\{ \Big[\sum_{m=-K/2}^{K/2-1} s_{\rm A}[m;n] e^{j2\pi \frac{m}{T_{\rm d}} t} g(t) \Big] e^{j2\pi f_{\rm c} t} \Big\}, \quad t \in [-T_{\rm cp}, T_{\rm d}] \tag{77}$$

[1]Note that the jamming signal could be optimized based on e.g., long term channel statistics. The secrecy rate would be different with a different jamming signal.

where $g(t)$ is a rectangular pulse-shaping window,

$$g(t) = \begin{cases} 1, & t \in [-T_{\mathrm{cp}}, T_{\mathrm{d}}], \\ 0, & \text{otherwise.} \end{cases} \tag{78}$$

Assume that the underwater channel for the nth block is modeled as:

$$h(\tau; n) = \sum_{p=1}^{N_{\mathrm{pa}}^{(n)}} A_p^{(n)} \delta\left(\tau - \tau_p^{(n)}\right) \tag{79}$$

where $N_{\mathrm{pa}}^{(n)}$ is the number of paths, $A_p^{(n)}$ and $\tau_p^{(n)}$ are the amplitude and delay of the pth path, respectively. In other words, the Doppler effect is not considered, and the results obtained are in an ideal case with calm channel conditions. There are three channels involved, $h_{\mathrm{AB}}(\tau; n)$, $h_{\mathrm{AE}}(\tau; n)$, and $h_{\mathrm{BE}}(\tau; n)$, which will be specified when used.

4.3.2 Receiver Processing at Bob

As shown in Fig. 23, denote the distances between Alice and Bob as d_{AB}. Let c denote the sound speed in water, $t_{\mathrm{A}}^{(n)}$ the starting transmission time of the nth block at Alice. Then the arrival time of signal at Bob from Alice, as Fig. 24(b) shows, is

$$\xi_{\mathrm{AB}}^{(n)} = t_{\mathrm{A}}^{(n)} + d_{\mathrm{AB}}/c, \quad t_{\mathrm{A}}^{(n)} = t_{\mathrm{A}}^{(1)} + (n-1)T_{\mathrm{bl}}. \tag{80}$$

The channel between Alice and Bob can be denoted as

$$h_{\mathrm{AB}}(\tau; n) = \sum_{p=1}^{N_{\mathrm{AB,pa}}^{(n)}} A_{\mathrm{AB},p}^{(n)} \delta\left(\tau - \tau_{\mathrm{AB},p}^{(n)}\right). \tag{81}$$

Suppose the received signal is perfect synchronized at the desirable start of each block. The received nth block passband signal at Bob for $t \in [0, T_{\mathrm{d}}]$ is

$$\tilde{z}_{\mathrm{B}}(t;n) = \tilde{y}_{\mathrm{AB}}(t + \xi_{\mathrm{AB}}^{(n)}; n) + \tilde{w}_{\mathrm{B}}(t;n), \tag{82}$$

where

$$\tilde{y}_{\mathrm{AB}}(t;n) = \sum_{p=1}^{N_{\mathrm{AB,pa}}^{(n)}} A_{\mathrm{AB},p}^{(n)} \tilde{x}_{\mathrm{A}} \left(t - \tau_{\mathrm{AB},p}^{(n)}; n \right). \tag{83}$$

and $\tilde{w}_{\mathrm{B}}(t;n)$ is the ambient noise for the nth block.

Taking the Fourier transform of (82), the frequency-domain measurement of $\tilde{z}_{\mathrm{B}}(t;n)$ on the mth subcarrier becomes

$$\begin{aligned} Z_{\mathrm{B}}[m;n] &= \int_0^{T_{\mathrm{d}}} \tilde{z}_{\mathrm{B}}(t;n) e^{-j2\pi f_m t} dt \\ &= H_{\mathrm{AB}}[m;n] s_{\mathrm{A}}[m;n] + W_{\mathrm{B}}[m;n]. \end{aligned} \tag{84}$$

where $H_{\mathrm{AB}}[m;n]$ is the channel frequency response on the mth subcarrier of the nth data block, defined as

$$H_{\mathrm{AB}}[m;n] = \int_0^{T_{\mathrm{d}}} h_{\mathrm{AB}}(\tau;n) e^{-j2\pi f_m t} dt, \tag{85}$$

and $W_{\mathrm{B}}[m;n]$ is the additive noise on the mth subcarrier of the nth block.

Assume that the additive noise on all the subcarriers is white Gaussian distributed $W_{\mathrm{B}}[m;n] \sim \mathcal{CN}(0, \sigma_{\mathrm{B,W}}^2)$, and each subcarrier has the same symbol energy σ_{S}^2. The mutual information available at Bob is

$$C_{\mathrm{B}} = \frac{1}{KN} \sum_{n=1}^{N} \sum_{m=-K/2}^{K/2-1} \log_2 \left(1 + \frac{|H_{\mathrm{AB}}[m;n]|^2 \sigma_{\mathrm{S}}^2}{\sigma_{\mathrm{B,W}}^2} \right). \tag{86}$$

4.3.3 Receiver Processing at Eve

The distances between Alice and Eve, and Bob and Eve are denoted as d_{AE} and d_{BE}, respectively as shown in Fig. 23. Denote $t_{\mathrm{B}}^{(n)}$ as the transmission start time of the nth block from Bob. The time-of-arrival of the nth block signal at Eve from Alice and Bob is

$$\xi_{\mathrm{AE}}^{(n)} = t_{\mathrm{A}}^{(n)} + d_{\mathrm{AE}}/c, \tag{87}$$

$$\xi_{\mathrm{BE}}^{(n)} = t_{\mathrm{B}}^{(n)} + d_{\mathrm{BE}}/c, \quad t_{\mathrm{B}}^{(n)} = t_{\mathrm{B}}^{(1)} + (n-1)T_{\mathrm{bl}}. \tag{88}$$

Denote the channel between Alice and Eve as $h_{\mathrm{AE}}(\tau; n)$, and the channel between Bob and Eve as $h_{\mathrm{BE}}(\tau; n)$,

$$h_{\mathrm{AE}}(\tau; n) = \sum_{p=1}^{N_{\mathrm{AE,pa}}^{(n)}} A_{\mathrm{AE},p}^{(n)} \delta\left(\tau - \tau_{\mathrm{AE},p}^{(n)}\right), \tag{89}$$

$$h_{\mathrm{BE}}(\tau; n) = \sum_{p=1}^{N_{\mathrm{BE,pa}}^{(n)}} A_{\mathrm{BE},p}^{(n)} \delta\left(\tau - \tau_{\mathrm{BE},p}^{(n)}\right). \tag{90}$$

Considering the time-of-arrival of data and jamming blocks, the received passband signal at Eve from Alice and Bob can be given by

$$\tilde{y}_{\mathrm{AE}}(t) = \sum_{n=1}^{N} \tilde{y}_{\mathrm{AE}}(t - \xi_{\mathrm{AE}}^{(n)}; n), \tag{91}$$

$$\tilde{y}_{\mathrm{BE}}(t) = \sum_{n=1}^{N+1} \tilde{y}_{\mathrm{BE}}(t - \xi_{\mathrm{BE}}^{(n)}; n), \tag{92}$$

and the nth received block as

$$\tilde{y}_{\mathrm{AE}}(t; n) = \sum_{p=1}^{N_{\mathrm{AE,pa}}^{(n)}} A_{\mathrm{AE},p}^{(n)} \tilde{x}_{\mathrm{A}}\left(t - \tau_{\mathrm{AE},p}^{(n)}; n\right), \tag{93}$$

$$\tilde{y}_{\mathrm{BE}}(t; n) = \sum_{p=1}^{N_{\mathrm{BE,pa}}^{(n)}} A_{\mathrm{BE},p}^{(n)} \tilde{x}_{\mathrm{B}}\left(t - \tau_{\mathrm{BE},p}^{(n)}; n\right), \tag{94}$$

where $\tilde{x}_{\mathrm{B}}(t;n)$ is the nth transmitted jamming block from Bob. Then the received signal at Eve in passband is

$$\tilde{y}_{\mathrm{E}}(t) = \tilde{y}_{\mathrm{AE}}(t) + \tilde{y}_{\mathrm{BE}}(t) + \tilde{w}_{\mathrm{E}}(t), \tag{95}$$

where $\tilde{w}_{\mathrm{E}}(t)$ is the ambient noise at Eve.

The received signal is synchronized via the preamble. For a specified nth data block at Eve, the truncated signal $\tilde{z}_{\mathrm{E}}(t;n)$ for $t \in [0, T_{\mathrm{d}}]$ can be given by

$$\begin{aligned}\tilde{z}_{\mathrm{E}}(t;n) &= \tilde{y}_{\mathrm{E}}(t + \xi_{\mathrm{AE}}^{(n)}; n) \\ &= \tilde{y}_{\mathrm{AE}}(t + \xi_{\mathrm{AE}}^{(n)}; n) + \sum_{j=1}^{N+1} \tilde{y}_{\mathrm{BE}}(t + \xi_{\mathrm{AE}}^{(n)}; j) + \tilde{w}_{\mathrm{E}}(t + \xi_{\mathrm{AE}}^{(n)}; n)\end{aligned} \tag{96}$$

where the first item is the eavesdropped nth block signal from Alice, and the second item is the jamming signal from Bob. Whether the jth block of jamming signal would interfere the nth data block depends on the location of Bob and Eve.

The $[0, T_{\mathrm{d}}]$ portion of the nth CP-OFDM block is used for decoding. By taking the Fourier transform of the truncated signal, the corresponding frequency-domain

measurement of $\tilde{z}_{\mathrm{E}}(t;n)$ on the mth subcarrier becomes

$$\begin{aligned} Z_{\mathrm{E}}[m;n] &= \int_0^{T_{\mathrm{d}}} \tilde{z}_{\mathrm{E}}(t;n) e^{-j2\pi f_m t} dt \\ &= \int_0^{T_{\mathrm{d}}} \tilde{y}_{\mathrm{AE}}(t+\xi_{\mathrm{AE}}^{(n)};n) e^{-j2\pi f_m t} dt \\ &+ \underbrace{\int_0^{T_{\mathrm{d}}} \sum_{j=1}^{N+1} \tilde{y}_{\mathrm{BE}}(t+\xi_{\mathrm{AE}}^{(n)};j) e^{-j2\pi f_m t} dt}_{:=I_{\mathrm{BE}}[m;n]} \\ &+ \underbrace{\int_0^{T_{\mathrm{d}}} \tilde{w}_{\mathrm{E}}^{(n)}(t+\xi_{\mathrm{AE}};n) e^{-j2\pi f_m t} dt}_{:=W_{\mathrm{E}}[m;n]} \\ &= H_{\mathrm{AE}}[m;n] s_{\mathrm{A}}[m;n] + I_{\mathrm{BE}}[m;n] + W_{\mathrm{E}}[m;n] \end{aligned} \tag{97}$$

where the channel frequency response on the mth subcarrier of the nth data block is

$$H_{\mathrm{AE}}[m;n] = \int_0^{T_{\mathrm{d}}} h_{\mathrm{AE}}(\tau;n) e^{-j2\pi f_m t} dt, \tag{98}$$

and the second item $I_{\mathrm{BE}}[m;n]$ denotes the interference and the last item $W_{\mathrm{E}}[m;n]$ represents the additive noise in frequency domain.

Assume the waveform of the transmitted jamming block follows white Gaussian distribution. According to the path-based channel model of (79), the path-based waveform of the received jamming block is still Gaussian distributed. The challenge here is to compute the variance of $I_{\mathrm{BE}}[m;n]$, which is denoted as $\sigma_{\mathrm{I}}^2[m;n]$.

Suppose that the power spectral density of the ambient noise at Eve is still white Gaussian distributed with $W_{\mathrm{E}}[m;n] \sim \mathcal{CN}(0, \sigma_{\mathrm{E,W}}^2)$. The received signal-to-interference-and-noise ratio (SINR) of the mth subcarrier of the nth data block at Eve can be written as

$$\mathrm{SINR}_{\mathrm{E}}[m;n] = \frac{|H_{\mathrm{AE}}[m;n]|^2 \sigma_{\mathrm{S}}^2}{\sigma_{\mathrm{I}}^2[m;n] + \sigma_{\mathrm{E,W}}^2}. \tag{99}$$

The mutual information available at Eve is

$$C_{\mathrm{E}} = \frac{1}{KN} \sum_{n=1}^{N} \sum_{m=-K/2}^{K/2-1} \log_2 \left(1 + \frac{|H_{\mathrm{AE}}[m;n]|^2 \sigma_{\mathrm{S}}^2}{\sigma_{\mathrm{I}}^2[m;n] + \sigma_{\mathrm{E,W}}^2} \right). \tag{100}$$

4.3.3.1 Interference Power Computation

Now let us look into jamming patterns at Eve. Fig. 26 shows the two cases that jamming happens. Case 1): the end time of the jth jamming block lies between the duration of the nth data block, $\xi_{\mathrm{AE}}^{(n)} + T_{\mathrm{cp}} < \xi_{\mathrm{BE}}^{(j)} + T_J + \tau_{\mathrm{max,BE}} < \xi_{\mathrm{AE}}^{(n)} + T_{\mathrm{bl}}$; Case 2): the nth data block covers the starting time of the jth jamming block, $\xi_{\mathrm{AE}}^{(n)} + T_{\mathrm{cp}} < \xi_{\mathrm{BE}}^{(j)} < \xi_{\mathrm{AE}}^{(n)} + T_{\mathrm{bl}}$. Combining the two cases, we can see the interference happens when $\xi_{\mathrm{AE}}^{(n)}$ and $\xi_{\mathrm{BE}}^{(j)}$ satisfy

$$T_{\mathrm{cp}} - T_{\mathrm{J}} - \tau_{\mathrm{max,BE}} < \xi_{\mathrm{BE}}^{(j)} - \xi_{\mathrm{AE}}^{(n)} < T_{\mathrm{bl}}. \tag{101}$$

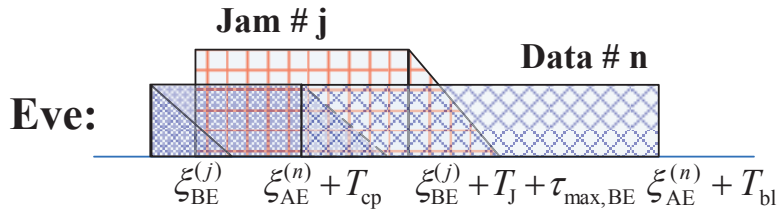
Although there are $N+1$ jamming blocks transmitted, at most there are two jamming blocks j and $j+1$ that can collide with the nth CP-OFDM data block.

Define $T_{\mathrm{I},p}^{(n,j)}$ as the time duration that the nth data block is overlapped by the pth path of the jth jamming block. Define an indicator function $L(\xi_{\mathrm{AE}}^{(n)}, \xi_{\mathrm{BE}}^{(j)})$ as

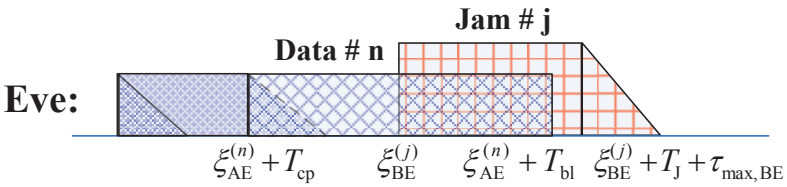
$$L(\xi_{\mathrm{AE}}^{(n)}, \xi_{\mathrm{BE}}^{(j)}) = \begin{cases} 1, & T_{\mathrm{cp}} - T_{\mathrm{J}} - \tau_{\mathrm{max,BE}} < (\xi_{\mathrm{BE}}^{(j)} - \xi_{\mathrm{AE}}^{(n)}) < T_{\mathrm{bl}} \\ 0, & \text{otherwise} \end{cases}. \tag{102}$$

Then $T_{\mathrm{I,p}}^{(n,j)}$ can be expressed as

$$\begin{aligned} T_{\mathrm{I},p}^{(n,j)} = \Big(\min \Big\{ & (\xi_{\mathrm{BE}}^{(j)} + T_{\mathrm{J}} + \tau_{\mathrm{BE},p}^{(j)}) - (\xi_{\mathrm{AE}}^{(n)} + T_{\mathrm{cp}}), \\ & (\xi_{\mathrm{AE}}^{(n)} + T_{\mathrm{bl}}) - (\xi_{\mathrm{BE}}^{(j)} + \tau_{\mathrm{BE},p}^{(j)}), T_{\mathrm{J}} \Big\} \Big) L(\xi_{\mathrm{AE}}^{(n)}, \xi_{\mathrm{BE}}^{(j)}). \end{aligned} \tag{103}$$



(a) Case 1



(b) Case 2

Figure 26: CP-OFDM jamming cases

For simplicity, we assume that the jamming power on all the subcarriers can be treated as approximately equal, due to potentially partial overlap between the jamming blocks and the data block. Hence,

$$\sigma_{\mathrm{I}}^2[m;n] \approx \sigma_{\mathrm{I}}^2[n] \propto \left(\sum_{j=1}^{N+1} \sum_{p=1}^{N_{\mathrm{BE,pa},j}} (A_{\mathrm{BE},p}^{(j)})^2 \frac{T_{\mathrm{I},p}^{(n,j)}}{T_{\mathrm{d}}} \right) \sigma_{\mathrm{J}}^2 \tag{104}$$

where σ_{J}^2 is the nominal variance if a jamming block of duration T_{d} is perfectly aligned and added to the the received block.

4.3.4 Secrecy Rate

In references [56, 69], the average secrecy rate for a multicarrier system is defined as

$$C_0 = \frac{1}{KN} \sum_{n=1}^{N} \sum_{m=-K/2}^{K/2-1} \Big[\log_2(1+\mathrm{SNR}_{\mathrm{B}}[m;n]) - \log_2(1+\mathrm{SINR}_{\mathrm{E}}[m;n]) \Big]^+, \tag{105}$$

where N is the number of data blocks within one packet. This definition is based on that the encoding is carried out on each subcarrier of block independently. If the information is encoded across frequencies in our CP-OFDM systems, the secrecy rate becomes

$$C_1 = \frac{1}{KN}\sum_{n=1}^{N}\left[\sum_{m=-K/2}^{K/2-1}\log_2(1+\mathrm{SNR}_{\mathrm{B}}[m;n]) - \log_2(1+\mathrm{SINR}_{\mathrm{E}}[m;n])\right]^{+}. \tag{106}$$

Assume the interference power is white Gaussian distributed across the K subcarriers. If we carry out encoding across blocks and subcarriers, the average secrecy rate of this multicarrier communication systems is defined as

$$C_2 = \frac{1}{KN}\left[\sum_{n=1}^{N}\sum_{m=-K/2}^{K/2-1}\log_2(1+\mathrm{SNR}_{\mathrm{B}}[m;n]) - \log_2(1+\mathrm{SINR}_{\mathrm{E}}[m;n])\right]^{+} \tag{107}$$

$$= \frac{1}{KN}\left[\sum_{n=1}^{N}\sum_{m=-K/2}^{K/2-1}\log_2\left(1+\frac{|H_{\mathrm{AB}}[m;n]|^2\sigma_{\mathrm{S}}^2}{\sigma_{\mathrm{W}}^2}\right) - \log_2\left(1+\frac{|H_{\mathrm{AE}}[m;n]|^2\sigma_{\mathrm{S}}^2}{\sigma_{\mathrm{I}}^2[m;n]+\sigma_{\mathrm{W}}^2}\right)\right]^{+}, \tag{108}$$

where the secrecy rate of the system is evaluated by averaging the secrecy rate aggregation of all CP-OFDM blocks. From the definition of the three kinds of secrecy rate, we can see $C_0 \geq C_1 \geq C_2$. In this chapter, we assume that the encoding process is implemented across blocks and frequency, and use (107) as the proper metric for secrecy rate.

4.4 Simulation Performance

A single-input single-output (SISO) CP-OFDM communication system is considered for simulation, with center frequency $f_{\mathrm{c}} = 13$ kHz, bandwidth $B = 9.77$ kHz, symbol duration $T = 104.86$ ms, and CP length of $T_{\mathrm{cp}} = 29.6$ ms. The CP-OFDM system has $K = 1024$ subcarriers in total. Assume the simulated sparse UWA channel has 15 discrete paths. The inter-arrival time of paths is exponentially distributed with mean of 1 ms, resulting a 15-ms channel delay spread on average. The amplitude of each path is Rayleigh distributed with an exponential power decay profile [52]. The UWA channels are assumed to follow block fading, where the channel does not change within each block transmission.

The evaluated area is of 3600 m $\times$ 3600 m, and divided into numbers of squares of 10 m $\times$ 10 m. The secrecy rate at the midpoint of the squares will be used to represent the performance of these squares, and the secrecy rate based on the geometry is obtained by interpolating these squares. Bob is located 1000 m away from Alice, where the coordinate of Alice is defined as (0,0), and Bob defined as (1000,0). The received SNR at Bob is set to be 10 dB when the destination is 1000 m away from Alice. The CP-OFDM data signal and jamming signal are scaled to have the same transmission power for performance comparison. And the white Gaussian noises at Bob and Eve are assumed to at the same power level.

4.4.1 Channel Propagation Model in Simulation

The channel propagation model in UWA communication [103] is similar to that in wireless communication [23, 24], but with different characteristics. Due to the absorption loss from water and the spreading loss of signal, the transmission loss $A(d, f)$ which depends on the transmission distance d and the carrier frequency f, is given by [103]

$$A(d, f) = A_0 d^{-\delta} a(f)^{-d} \tag{109}$$

where A_0 is the normalizing constant, the exponent δ models the geometrical spreading effect, and $a(f)$ represents the absorption coefficient at the frequency f. Empirically, the spreading factor is $\delta = 1.5$. The equation of one-way transmission loss (TL) is expressed as

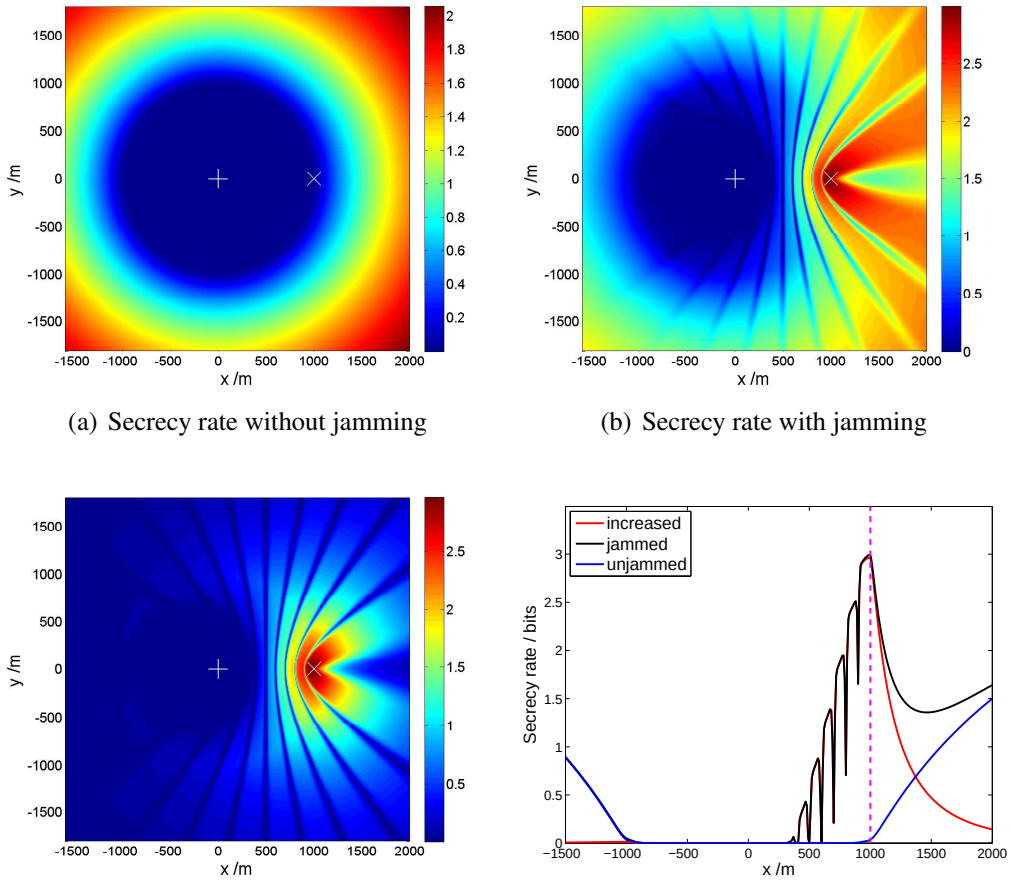
$$\text{TL}(d, f) = 10 \log A(d, f)/A_0 = 10\delta \cdot \log(10^3 d) + \alpha(f)d, \tag{110}$$

where TL is in dB, and d is in km. According to Thorp's formula, the absorption coefficient $a(f)$ above a few hundred Hz is approximated as [103]

$$\alpha(f) = 10 \log a(f) = 0.11 \frac{f^2}{1 + f^2} + 44 \frac{f^2}{4100 + f^2} + 2.75 \times 10^{-4} f^2 + 0.003 \tag{111}$$

where the metric of $\alpha(f)$ is in $\mathrm{dB/km}$, and f in kHz.

Approximate the transmission loss of the underwater acoustic channel as a constant within the bandwidth, since the variation of TL within a certain bandwidth B is small when the transmission distance is below 5 km [103]. The average channel strength for



(a) Secrecy rate without jamming

(b) Secrecy rate with jamming

(c) Increased secrecy rate with jamming

(d) Profile of secrecy rate

Figure 27: Geometry of secrecy rate with standard jamming power, 1000 m distance between Alice and Bob, 10 jamming blocks within one frame, $f_{\mathrm{c}} = 13$ kHz, jamming length of 24.6 ms, worked as the reference ("+": Alice; "×": Bob).

a multipath channel as in (79) is approximated by

$$E\left\{\sum_{p=1}^{N_{\mathrm{pa}}} A_p^2\right\} \propto 10^{-\frac{\mathrm{TL}(d,f_{\mathrm{c}})}{10}} \tag{112}$$

where d is the line-of-sight distance between transmitter and receiver.

4.4.2 Performance Evaluation

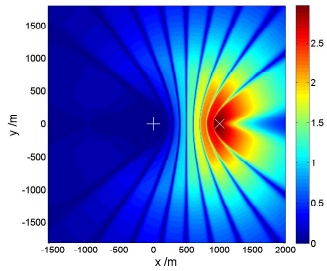
Fig. 27 shows the secrecy rate based on geometry of Eve with the same data and jamming transmission power at Alice and Bob, whose distance is 1000 m. Each packet consists of 10 CP-OFDM blocks. Assume the maximal delay spread of $h_{\mathrm{BB}}(t;n)$ is 5 ms, then the jamming length is 24.6 ms where 5 ms of CP duration is used for the self protection of Bob. All the CP-OFDM data signals and jamming signals are with the 13 kHz center frequency. Fig. 27(a) shows the secrecy rate without jamming. We can see the contour of the secrecy rate is a ring, which is zero when Eve lies in the circle of radius 1000 m, and increases as the distance goes up. With the help of half duplex jamming system of Bob, we can see from Fig. 27(b) that the zero secrecy rate shadow becomes a shell-like pattern. There are numbers of parabola-like shadows, since the most part of jamming signal overlaps the CP part instead of data part of blocks. Fig. 27(c) shows the increased secrecy rate from the perspective of geometry. We can see the area near Bob can provide much larger secrecy rate since the attenuation of jamming power is small, and the left side of Alice is less secure. Fig. 27(d) shows the profile of secrecy rate when Eve is on the line of Alice and Bob. We can see the increased secrecy rate decreases monotonously when the distance d_{AE} is above 1000 m, and increases with a large oscillation whose period is about 100 m when Eve gets close to Bob. The maximal increased average secrecy rate is 3 bits, which depends on the received SNR at Bob. The null of the oscillation happens periodically when

$2|d_{\mathrm{AE}} - d_{\mathrm{BE}}|/c = nT_{\mathrm{bl}}$, which leads to the least overlapping. The same phenomenon can be found in Fig. 28(c), 28(f), 28(i), and 28(l).

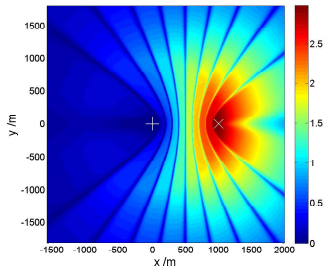
Since the jamming power, the number of jamming blocks within one packet, the center frequency f_{c} of the system, and the jamming duration T_{J} affect the overlapping duration and interference power within a data block, Fig. 28 shows their impact on the performance of the increased secrecy rate in the half duplex jamming system. We take Fig. 27 as the reference for performance comparison.

- *Jamming Power*: Fig. 28(a) and 28(b) indicate that as the jamming power increases, the bright area becomes larger, which implies the secrecy rate is increased. And we can still see ten parabola-like curves between Alice and Bob whose patterns do not change. Fig. 28(c) demonstrates increasing jamming power will enlarge the secrecy rate when Eve is on the right side of Alice.

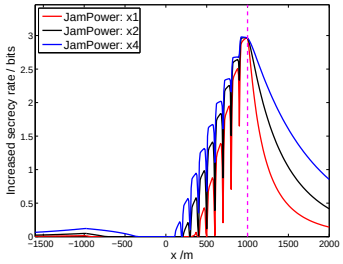
- *Number of jamming blocks within a packet*: Fig. 28(d) shows the performance with 5 data blocks within a packet, where the increased secrecy rate of the left plane is near zero, and 5 parabola-like curves appear on the right plane. When there are 20 data blocks within a packet, the area of increased secrecy rate is larger as Fig. 28(e) shows, since it provides longer data duration for the protection of overlap from Bob. However, Fig. 28(f) shows the increase of block number within a packet only increases the secrecy rate when Eve is between Alice and Bob. When Eve is on the right of Bob, increasing block number will not increase secrecy rate because all the blocks have the same overlapping pattern.



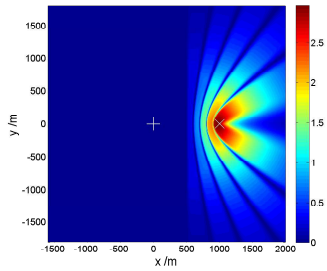
(a) Two times of jamming power



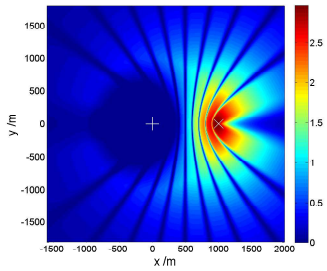
(b) Four times of jamming power



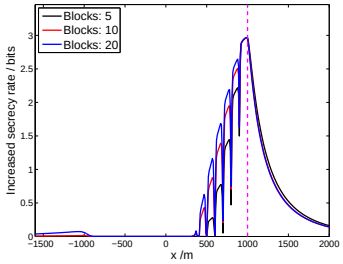
(c) Profile with different jamming powers



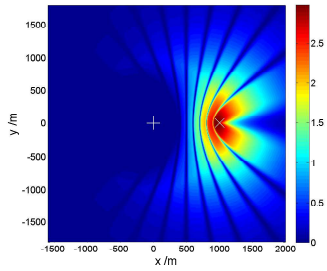
(d) 5 jamming blocks within one packet



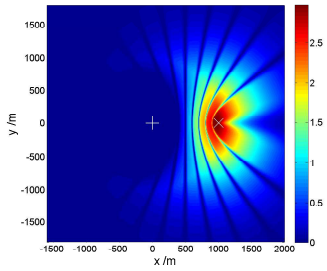
(e) 20 jamming blocks within one packet



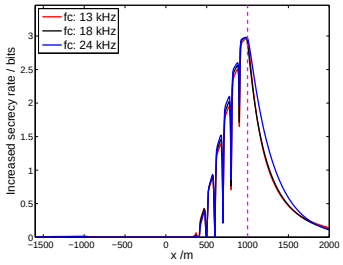
(f) Profile with different number of jamming blocks within one packet



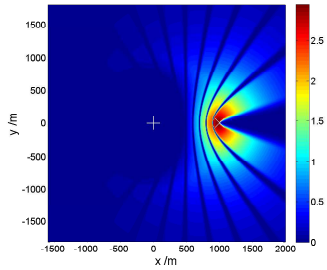
(g) Center frequency: 18 kHz



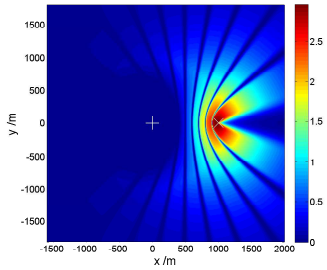
(h) Center frequency: 24 kHz



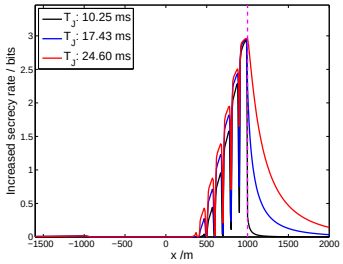
(i) Profile with different center frequencies



(j) Jamming lengths: 10.25 ms



(k) Jamming lengths: 17.43 ms



(l) Profile with different jamming lengths

Figure 28: Geometry of increased secrecy rate with different parameters ("+": Alice; "×": Bob).

- *Center frequency*: Fig. 28(g) and 28(h) show that the performance of increased secrecy rate under different center frequencies, the bright area is like a peacock showing the tail, and we cannot see much difference between these two figures. Fig. 28(i) indicates increasing the center frequency will not improve the increased secrecy rate. However, Fig. 29 shows that the unjammed and jammed secrecy rate will increase as the center frequency increases due to larger attenuation brought by higher center frequency. However, if the center frequency becomes too large, the assumption that the attenuation within the bandwidth is constant may not be true.

- *Jamming length*: Fig. 28(j) and Fig. 28(k) show that as the duration of jamming signal increases, the one with longer duration will cover a larger area of increased secrecy rate. Fig. 28(l) shows the increase of jamming duration improves the increased secrecy rate remarkably when Eve is on the right of Bob. Specifically when the jamming length is 10.25 ms, there would be some locations with no increase of secrecy rate, this is due to the length of jamming block plus the channel length is smaller than the CP length, resulting in no interference.

4.5 Conclusion

This chapter proposed a novel jamming approach for an underwater acoustic communication system with half-duplex transceivers. The receiver sends out jamming signals during the guard intervals between neighboring blocks, which will collide with

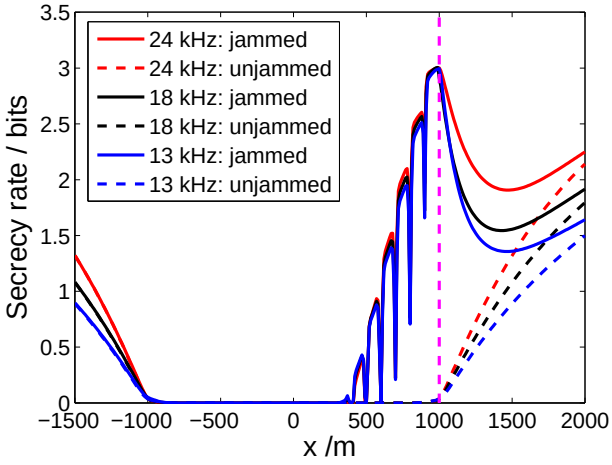


Figure 29: Profile of jammed and unjammed secrecy rate with different center frequencies.

the data blocks at the eavesdropper. We have simulated the system performance with various parameters. Our results have shown that this new protocol can increase the secrecy rate of the system as expected and is feasible for implementation.

Chapter 5

Conclusions

The work in this dissertation aims to improve physical layer security in UWA communication systems. Up to now, limited investigation has been done in this topic. The dissertation started from UWA acoustic channel estimation, due to its fundamental role in physical layer security. To set a proper regularization parameter in sparse recovery algorithms for channel estimation, we proposed a data-driven sparsity learning approach which can tune the regularization parameter adaptively. Thus, it can achieve nearly the same performance as that of the best fixed regularization parameter. To secure UWA communications by secret keys, a secret key generation protocol based on the CFR in OFDM system was proposed by exploiting the reciprocity of mutual channels. We also investigated the half-duplex jamming for block communications in UWA systems, where the self-protection jamming protocols were proposed by enjoying the benefit from the large propagation delays of UWA channels. The contributions of the dissertation are as follows.

- *Sparse channel estimation:* Instead of setting the regularization parameter in the sparse recovery algorithms empirically, we proposed a data-driven sparsity learning method based on the LMMSE equalizer to tune the regularization parameter adaptively. The decoding performance of different L_q algorithms in the ICI-ignorant and ICI-aware OFDM receivers were compared with simulated and experimental data from SPACE08. The result showed it achieves the near best and robust performance as the best fixed regularization parameter.

- *Secret key generation:* To counteract information eavesdropping in UWA systems, a protocol that can generate secret keys dynamically based on the CFR was developed, by exploiting the channel reciprocity and randomness at the physical layer. Based on the lake test results that the correlation between mutual channels is low, we incorporated two modules into the protocol for performance improvement.

- *Half-duplex self-protection jamming:* To improve the secrecy rate of block transmissions in UWA channels, we proposed a self-protection jamming approach, which relies on the legitimate receiver instead of extra helpers, to generate interference at the eavesdropper without affecting his/her own reception by exploring the large propagation delays.

Bibliography

[1] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[2] S. Al-Dharrab, M. Uysal, and T. M. Duman, "Cooperative underwater acoustic communications," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 146–153, Jul. 2013.

[3] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[4] AquaSeNT, "OFDM Acoustic Modem," http://www.aquasent.com/.

[5] C. D. Austin, R. Moses, J. Ash, and E. Ertin, "On the relation between sparse reconstruction and parameter estimation with model order selection," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 3, pp. 560–570, Jun. 2010.

[6] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Gaithersburg, MD, Tech. Rep., Sep. 2010.

[7] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[8] O. Batu and M. Cetin, "Parameter selection in sparsity-driven SAR imaging," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, no. 4, pp. 3040–3050, Oct. 2011.

[9] A. Beck and M. Teboulle, "A fast iterative shrinkage-thresholding algorithm for linear inverse problems," *SIAM Journal on Imaging Sciences*, vol. 2, no. 1, pp. 183–202, Mar. 2009.

[10] C. R. Berger, J. P. Gomes, and J. M. F. Moura, "Study of pilot designs for cyclic-prefix OFDM on time-varying and sparse underwater acoustic channels," in *Proc. of MTS/IEEE OCEANS Conf.*, Santander, Spain, Jun. 2011.

[11] C. R. Berger, S. Zhou, J. Preisig, and P. Willett, "Sparse channel estimation for multicarrier underwater acoustic communication: From subspace methods to compressed sensing," *IEEE Trans. Signal Processing*, vol. 58, no. 3, pp. 1708–1721, Mar. 2010.

[12] C. Bilen, I. Selesnick, Y. Wang, R. Otazo, D. Kim, L. Axel, and D. Sodickson, "On compressed sensing in parallel MRI of cardiac perfusion using temporal wavelet and TV regularization," in *Proc. of IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, Mar. 2010, pp. 630–633.

[13] J. M. Bioucas-Dias and M. A. Figueiredo, "A new TwIST: two-step iterative shrinkage/thresholding algorithms for image restoration," *IEEE Transactions on Image Processing*, vol. 16, no. 12, pp. 2992–3004, Dec. 2007.

[14] M. Bloch and J. Barros, *Physical Layer Security From Information Theory to Security Engineering*. Cambridge University Press, Oct. 2011.

[15] A. M. Bruckstein, D. L. Donoho, and M. Elad, "From sparse solutions of systems of equations to sparse modeling of signals and images," *SIAM Reviews*, vol. 51, no. 1, pp. 34–81, Feb. 2009.

[16] S.-H. Byun, W. Seong, and S.-M. Kim, "Sparse underwater acoustic channel parameter estimation using a wideband receiver array," *IEEE Journal of Oceanic Engineering*, vol. 38, no. 4, pp. 718–729, Oct. 2013.

[17] X. Cai, L. Wan, Y. Huang, S. Zhou, and Z. Shi, "Further results on multicarrier MFSK based underwater acoustic communications," *Elsevier Journal on Physical Communication*, vol. 18, pp. 15–27, Mar. 2016.

[18] Ö. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE communications letters*, vol. 18, no. 6, pp. 1075–1078, Jun. 2014.

[19] J. Chen, J.-H. Cui, and L. Wang, "Energy-adaptive modulation for RF power management under renewable energy," in *IEEE Workshop on Signal Processing Systems (SiPS)*, 2012, pp. 173–178.

[20] ——, "RF power management via energy-adaptive modulation for self-powered systems," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 9, pp. 1931–1935, 2015.

[21] J. Chen and L. Wang, "Energy-adaptive signal processing under renewable energy," *Journal of Signal Processing Systems*, pp. 1–14, 2015.

[22] ——, "Low-power LDPC decoder design exploiting memory error statistics," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*, 2015, pp. 171–176.

[23] J. Chen, D. Zhao, and L. Wang, "Link and energy adaptive UWB-based embedded sensing with renewable energy," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2013, pp. 1825–1828.

[24] ——, "Self-sustained UWB sensing: A link and energy adaptive approach," *Journal of Signal Processing Systems*, pp. 1–11, 2015.

[25] S. Chen, J. Chen, D. Forte, J. Di, M. Tehranipoor, and L. Wang, "Chip-level anti-reverse engineering using transformable interconnects," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*, 2015, pp. 109–114.

[26] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications Surveys Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[27] Y. Chen, "Superimposed pilots based secure communications for multiple antenna system," in *Proc. of the Asilomar Conference on Signals, Systems and Computers*, Nov. 2014.

[28] X. Cheng, M. Wen, X. Cheng, L. Yang, and Z. Xu, "Effective self-cancellation of intercarrier interference for OFDM underwater acoustic communications," in *Proceedings of the International Conference on UnderWater Networks and Systems (WUWNet)*, New York, NY, USA, Nov. 2013, pp. 33:1–33:5.

[29] M. Chitre, S. H. Ong, and J. Potter, "Performance of coded OFDM in very shallow water channels and snapping shrimp noise," in *Proc. of MTS/IEEE OCEANS Conf.*, vol. 2, 2005, pp. 996–1001.

[30] M. Chitre, M. Motani, and S. Shahabudeen, "Throughput of networks with large propagation delays," *IEEE Journal of Oceanic Engineering*, vol. 37, no. 4, pp. 645–658, Oct. 2012.

[31] T.-H. Chou, S. Draper, and A. Sayeed, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Jun. 2010, pp. 2518–2522.

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

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

[34] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *IEEE/SP 15th Workshop on Statistical Signal Processing*, Aug. 2009, pp. 417–420.

[35] ——, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[36] G. F. Edelmann, T. Akal, W. S. Hodgkiss, S. Kim, W. A. Kuperman, and H. C. Song, "An initial demonstration of underwater acoustic communications using time reversal," *IEEE J. Oceanic Eng.*, vol. 31, no. 3, pp. 602–609, Jul. 2002.

[37] T. H. Eggen, A. B. Baggeroer, and J. C. Preisig, "Communication over Doppler spread channels. Part I: Channel and receiver presentation," *IEEE Journal of Oceanic Engineering*, vol. 25, no. 1, pp. 62–71, Jan. 2000.

[38] Y. El Hajj Shehadeh and D. Hogrefe, "An optimal guard-intervals based mechanism for key generation from multipath wireless channels," in *Proc. of International Conference on New Technologies, Mobility and Security (NTMS)*, Feb. 2011, pp. 1–5.

[39] J. J. Fuchs, "More on sparse representations in arbitrary bases," *IEEE Transactions on Information Theory*, vol. 50, pp. 1341–1344, Jun. 2004.

[40] P. J. Gendron, "Orthogonal frequency division multiplexing with on-off-keying: Noncoherent performance bounds, receiver design and experimental results," *U.S. Navy Journal of Underwater Acoustics*, vol. 56, no. 2, pp. 267–300, Apr. 2006.

[41] A. Glavieux, P. Cochet, and A. Picart, "Orthogonal frequency division multiplexing with BFSK modulation in frequency selective rayleigh and rician fading channels," *IEEE Transactions on Communications*, vol. 42, no. 234, pp. 1919–1928, Feb. 1994.

[42] J. Gomes, A. Silva, and S. Jesus, "Experimental assessment of time-reversed OFDM underwater communications," *J. Acoust. Soc. Am.*, vol. 123, no. 5, p. 38913891, 2008.

[43] R. Guillaume, A. Mueller, C. T. Zenger, C. Paar, and A. Czylwik, "Fair comparison and evaluation of quantization schemes for PHY-based key generation," in *Proc. of 18th International OFDM Workshop (InOWo'14)*, Aug. 2014, pp. 1–5.

[44] A. S. Gupta and J. Preisig, "A geometric mixed norm approach to shallow water acoustic channel estimation and tracking," *Physical Communication*, vol. 5, no. 2, pp. 119–128, Jun. 2012.

[45] B. Gurakan and S. Ulukus, "Energy harvesting cooperative diamond channel," in *2015 IEEE International Symposium on Information Theory (ISIT)*, Jun. 2015, pp. 2732–2736.

[46] J. Hao, Y. Zheng, J. Wang, and J. Song, "Dual PN padding TDS-OFDM for underwater acoustic communication," in *MTS/IEEE OCEANS*, Oct. 2012, pp. 1–4.

[47] C. He, Q. Zhang, J. Huang, J. Han, and W. Shi, "Single-carrier block transmission in time reversal shortened underwater acoustic channels," in *Proc. of the ACM Intl. Workshop on Underwater Networks (WUWNet)*, Nov. 2013.

[48] J. Huang, C. R. Berger, S. Zhou, and J. Huang, "Comparison of basis pursuit algorithms for sparse channel estimation in underwater acoustic OFDM," in *Proc. of OCEANS*, Sydney, Australia, May 2010, pp. 1–6.

[49] J. Huang, S. Zhou, J. Huang, J. Preisig, L. Freitag, and P. Willett, "Progressive intercarrier and co-channel interference mitigation for underwater acoustic multi-input multi-output orthogonal frequency-division multiplexing," *Wireless Communications and Mobile Computing*, 2012.

[50] J. Huang, S. Zhou, J. Huang, C. Berger, and P. Willett, "Progressive inter-carrier interference equalization for OFDM transmission over time-varying underwater acoustic channels," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 8, pp. 1524–1536, Dec. 2011.

[51] J. Huang, S. Zhou, and P. Willett, "Nonbinary LDPC coding for multicarrier underwater acoustic communication," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 9, pp. 1684–1696, Dec. 2008.

[52] Y. Huang, L. Wan, S. Zhou, Z. Wang, and J. Huang, "Comparison of sparse recovery algorithms for channel estimation in underwater acoustic OFDM with data-driven sparsity learning," *Elsevier Journal on Physical Communication*, vol. 13, pp. 156–167, Dec. 2014.

[53] Y. Huang, P. Xiao, S. Zhou, and Z. Shi, "A half-duplex self-protection jamming approach for improving secrecy of block transmissions in underwater acoustic channels," *IEEE Sensors Journal*, vol. 16, no. 11, pp. 4100–4109, Jun. 2016.

[54] Y. Huang, S. Zhou, Z. Shi, and L. Lai, "Experimental study of secret key generation in underwater acoustic channels," in *Proc. of the Asilomar Conference on Signals, Systems and Computers*, Nov. 2014.

[55] ——, "Channel frequency response based secret key generation in underwater acoustic systems," *IEEE Transactions on Wireless Communications*, May 2016 (Accepted).

[56] E. A. Jorswieck, A. Wolf, and S. Gerbracht, *Secrecy on the physical layer in wireless networks*. INTECH Open Access Publisher, 2010.

[57] H. Ju and R. Zhang, "Optimal resource allocation in full-duplex wireless-powered communication network," *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3528–3540, Oct. 2014.

[58] S.-J. Kim, K. Koh, M. Lustig, S. Boyd, and D. Gorinevsky, "An interior-point method for large-scale l 1-regularized least squares," *IEEE Journal of Selected Topics in Signal Processing*, vol. 1, no. 4, pp. 606–617, Dec. 2007.

[59] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[60] G. Leus and P. A. V. Walree, "Multiband OFDM for covert acoustic communications," *IEEE J. Select. Areas Commun.*, vol. 26, no. 9, pp. 1662–1673, Dec. 2008.

[61] B. Li, S. Zhou, M. Stojanovic, L. Freitag, and P. Willett, "Multicarrier communication over underwater acoustic channels with nonuniform Doppler shifts," *IEEE Journal of Oceanic Engineering*, vol. 33, no. 2, pp. 198–209, Apr. 2008.

[62] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, "Security and privacy in localization for underwater sensor networks," *IEEE Communications Magazine*, vol. 53, no. 11, pp. 56–62, Nov. 2015.

[63] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[64] W. Li and J. C. Preisig, "Estimation of rapidly time-varying sparse channels," *IEEE Journal of Oceanic Engineering*, vol. 32, no. 4, pp. 927–939, Oct. 2007.

[65] J. Ling and J. Li, "Gibbs-sampler-based semiblind equalizer in underwater acoustic communications," *IEEE Journal of Oceanic Engineering*, vol. 37, no. 1, pp. 1–13, Jan. 2012.

[66] J. Ling, T. Yardibi, X. Su, H. He, and J. Li, "Enhanced channel estimation and symbol detection for high speed MIMO underwater acoustic communications," *The Journal of the Acoustical Society of America*, vol. 125, no. 5, pp. 3067–3078, 2009.

[67] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. of IEEE INFOCOM*, Apr. 2013, pp. 3048–3056.

[68] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2820–2835, Dec. 2014.

[69] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer Publishing Company, 2009.

[70] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[71] Z. Liu and T. Yang, "On overhead reduction in time-reversed OFDM underwater acoustic communications," *IEEE Journal of Oceanic Engineering*, vol. 39, no. 4, pp. 788–800, Oct. 2014.

[72] Q. Lu, Y. Huang, Z. Wang, and S. Zhou, "Characterization and receiver design for underwater acoustic channels with large Doppler spread," in *Proc. of IEEE/MTS OCEANS conference*, Oct. 2015, pp. 23–27.

[73] S. Luo, J. Li, and A. Petropulu, "Uncoordinated cooperative jamming for secret communications," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1081–1090, Jul. 2013.

[74] Y. Luo, L. Pu, Z. Peng, Z.-J. Shi, and J.-H. Cui, "RSS-based secret key generation in underwater acoustic networks: advantages, challenges and performance improvements," in *Techical Report at UCONN CSE*, 2014; doi=UbiNet-TR14-01.

[75] Y. Luo, L. Pu, Z. Peng, Z. Zhou, and J.-H. Cui, "An efficient MAC protocol for underwater multi-user uplink communication networks," *Ad Hoc Networks*, vol. 34, pp. 75–91, 2015.

[76] Y. Luo, L. Pu, M. Zuba, Z. Peng, and J.-H. Cui, "Challenges and opportunities of underwater cognitive acoustic networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 2, pp. 198–211, 2014.

[77] S. Mason, C. Berger, S. Zhou, and P. Willett, "Detection, synchronization, and Doppler scale estimation with multicarrier waveforms in underwater acoustic communication," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 9, pp. 1638–1649, Dec. 2008.

[78] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on mobile computing and networking*, Mar. 2008, pp. 128–139.

[79] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[80] A. Morozov and J. Preisig, "Underwater acoustic communications with multicarrier modulation," in *OCEANS*, Sept 2006, pp. 1–6.

[81] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 1, Jan. 2014.

[82] Y. Nesterov, "Primal-dual subgradient methods for convex problems," *Mathematical programming*, vol. 120, no. 1, pp. 221–259, Jun. 2009.

[83] C. C. Paige and M. A. Saunders, "LSQR: An algorithm for sparse linear equations and sparse least squares," *ACM Transactions on Mathematical Software (TOMS)*, vol. 8, no. 1, pp. 43–71, Jun. 1982.

[84] A. Panahi and M. Viberg, "Maximum a posteriori based regularization parameter selection," in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2011, pp. 2452–2455.

[85] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[86] ——, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, Jan 2010.

[87] S. Pouryazdian, S. Beheshti, and S. Krishnan, "Minimum noiseless description length (MNDL) based regularization parameter selection," in *Proc. of the 11th International Conference on Information Science, Signal Processing and their Applications (ISSPA)*, 2012, pp. 1341–1346.

[88] L. Pu, Y. Luo, H. Mo, S. Le, Z. Peng, J.-H. Cui, and Z. Jiang, "Comparing underwater mac protocols in real sea experiments," *Computer Communications*, vol. 56, pp. 47–59, 2015.

[89] L. Pu, Y. Luo, Y. Zhu, Z. Peng, J.-H. Cui, S. Khare, L. Wang, and B. Liu, "Impact of real modem characteristics on practical underwater MAC design," in *Proceedings of IEEE OCEANS-Yeosu*, 2012, pp. 1–6.

[90] C. Qi, L. Wu, and X. Wang, "Underwater acoustic channel estimation via complex homotopy," in *IEEE International Conference on Communications (ICC)*, 2012, pp. 3821–3825.

[91] K. Qiu and A. Dogandzic, "Sparse signal reconstruction via ECME hard thresholding," *IEEE Transactions on Signal Processing*, vol. 60, no. 9, pp. 4551–4569, Sep. 2012.

[92] F. Qu and L. Yang, "Basis expansion model for underwater acoustic channels?" in *OCEANS*, vol. 1, no. 7, Sep. 2008, pp. 15–18.

[93] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, "A survey on chip to system reverse engineering," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 13, no. 1, p. 6, 2016.

[94] A. Radosevic, R. Ahmed, T. M. Duman, J. G. Proakis, and M. Stojanovic, "Adaptive OFDM modulation for underwater acoustic communications: Design considerations and experimental results," *IEEE Journal of Oceanic Engineering*, vol. 39, no. 2, pp. 357–370, Apr. 2014.

[95] S. Ramani, T. Blu, and M. Unser, "Monte-carlo SURE: A black-box optimization of regularization parameters for general denoising algorithms," *IEEE Transactions on Image Processing*, vol. 17, no. 9, pp. 1540–1554, Sep. 2008.

[96] B. Rao, K. Engan, S. Cotter, J. Palmer, and K. Kreutz-Delgado, "Subset selection in noise based on diversity measure minimization," *IEEE Transactions on Signal Processing*, vol. 51, no. 3, pp. 760–770, Mar. 2003.

[97] G. Revadigar, C. Javali, H. J. Asghar, K. B. Rasmussen, and S. Jha, "Mobility independent secret key generation for wearable health-care devices," in *Proceedings of the 10th EAI International Conference on Body Area Networks*, 2015, pp. 294–300.

[98] C. Shahriar, M. La Pan, M. Lichtman, T. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. Reed, "Phy-layer resiliency in OFDM communications: A tutorial," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 292–314, 2015.

[99] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[100] Y. E. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Security and Communication Networks*, vol. 8, no. 2, Mar. 2014.

[101] M. Stojanovic, "Low complexity OFDM detector for underwater acoustic channels," in *OCEANS 2006*, Sep. 2006, pp. 1–6.

[102] ——, "OFDM for underwater acoustic communications: Adaptive synchronization and sparse channel estimation," in *Proceedings of International Conference on Acoustics, Speech and Signal Proc.*, Mar. 2008, pp. 5288–5291.

[103] ——, "On the relationship between transmission power and capacity of an underwater acoustic communication channel," in *Proceedings of the international workshop on Underwater networks*, Apr. 2008, pp. 1–6.

[104] M. Stojanovic and J. Preisig, "Underwater acoustic communication channels: Propagation models and statistical characterization," *IEEE Communications Magazine*, vol. 47, no. 1, pp. 84–89, Jan. 2009.

[105] Y. Su, Y. Zhang, S. Le, H. Mo, L. Wei, Y. Huang, Z. Peng, and J. Cui, "A versatile lab testbed for underwater sensor networks," in *Proc. of IEEE/MTS OCEANS conference*, vol. 1, no. 5, Sep. 2013.

[106] J. Tao and Y. R. Zheng, "Turbo detection for MIMO-OFDM underwater acoustic communications," in *International Journal of Wireless Information Networks*, vol. 20, no. 1, Hampton Roads, VA, Mar. 2013, pp. 27–38.

[107] J. Tropp and A. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.

[108] M. Tuchler, A. Singer, and R. Koetter, "Minimum mean squared error equalization using a priori information," *IEEE Transactions on Signal Processing*, vol. 50, no. 3, pp. 673–683, Mar. 2002.

[109] L. Wan, Z. Wang, S. Zhou, T. C. Yang, and Z. Shi, "Performance comparison of Doppler scale estimation methods for underwater acoustic OFDM," *Journal of Electrical and Computer Engineering*, 2012.

[110] L. Wan, H. Zhou, X. Xu, Y. Huang, S. Zhou, Z. Shi, and J.-H. Cui, "Adaptive modulation and coding for underwater acoustic OFDM," *IEEE Journal of Oceanic Engineering*, vol. 40, no. 2, pp. 327–336, Apr. 2015.

[111] ——, "Field tests of adaptive modulation and coding for underwater acoustic OFDM," in *Proceedings of the 8th ACM International Workshop on Underwater Networks and Systems*, Nov. 11-13, 2013.

[112] C. Wang, Z. Wang, and S. Nooshabadi, "Signal alignment for secure underwater coordinated multipoint transmissions," in *IEEE Conference on Communications and Network Security (CNS)*, Oct. 2014, pp. 145–150.

[113] L. Wang, J. Tao, C. Xiao, and T. Yang, "Low-complexity turbo detection for single-carrier low-density parity-check-coded multiple-input multiple-output underwater acoustic communications," *Wireless Communications and Mobile Computing*, vol. 13, no. 4, pp. 439–450, Jul. 2013.

[114] X. Wang and H. Poor, "Iterative (turbo) soft interference cancellation and decoding for coded CDMA," *IEEE Transactions on Communications*, vol. 47, no. 7, pp. 1046–1061, Jul. 1999.

[115] Z. Wang, S. Zhou, J. Catipovic, and P. Willett, "Asynchronous multiuser reception for OFDM in underwater acoustic communications," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1050–1061, Mar. 2013.

[116] M. Wen, X. Cheng, X. Cheng, L. Yang, D. Duan, and B. Jiao, "Effective intercarrier interference reduction techniques for OFDM underwater acoustic communications," in *Proceedings of the 47th Asilomar Conference on Signals, Systems and Computers*, Nov. 2013, pp. 93–97.

[117] M. Wilhelm, I. Martinovic, and J. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1779–1790, Sep. 2013.

[118] S. Wright, R. Nowak, and M. Figueiredo, "Sparse reconstruction by separable approximation," *IEEE Transactions on Signal Processing*, vol. 57, no. 7, pp. 2479–2493, Jul. 2009.

[119] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[120] X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, "A secret key generation method based on CSI in OFDM-FDD system," in *Proc. of IEEE Globecom Workshops*, Dec. 2013, pp. 1297–1302.

[121] A. D. Wyner, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[122] W. Xi, X.-Y. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, "KEEP: Fast secret key extraction protocol for D2D communication," in *Proc. of International Symposium of Quality of Service (IWQoS)*, May 2014, pp. 350–359.

[123] X. Xu, Z. Wang, S. Zhou, and L. Wan, "Parameterizing both path amplitude and delay variations of underwater acoustic channels for block decoding of orthogonal frequency division multiplexing," *The Journal of the Acoustical Society of America*, vol. 131, no. 6, pp. 4672–4679, 2012.

[124] Z. Xu, X. Chang, F. Xu, and H. Zhang, "$l_{1/2}$ regularization: A thresholding representation theory and a fast solver," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 23, no. 7, pp. 1013–1027, Jul. 2012.

[125] H. Yan, L. Wan, S. Zhou, Z. Shi, J. H. Cui, J. Huang, and H. Zhou, "DSP based receiver implementation for OFDM acoustic modems," *Physical Communication*, vol. 5, no. 1, pp. 22–32, Mar. 2012.

[126] T. C. Yang, "Temporal resolutions of time-reversal and passive-phase conjugation for underwater acoustic communications," *IEEE Journal of Oceanic Engineering*, vol. 28, no. 2, pp. 229–245, Apr. 2003.

[127] S. Yasukawa, H. Iwai, and H. Sasaoka, "Adaptive key generation in secret key agreement scheme based on the channel characteristics in OFDM," in *Proc. of International Symposium on Information Theory and Its Applications (ISITA)*, Dec. 2008, pp. 1–6.

[128] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[129] H. Zeng, Y. T. Hou, Y. Shi, W. Lou, S. Kompella, and S. F. Midkiff, "Shark-IA: An interference alignment algorithm for multi-hop underwater acoustic networks with large propagation delays," in *Proceedings of the International Conference on UnderWater Networks and Systems (WUWNet)*, Nov. 12-14, 2014, pp. 6:1–6:8.

[130] J. S. Zeng, J. Fang, and Z. B. Xu, "Sparse SAR imaging based on $l_{1/2}$ regularization," *Science China Information Sciences*, vol. 55, no. 8, pp. 1755–1775, Aug. 2012.

[131] C. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," in *Workshop on Wireless Communication Security at the Physical Layer*, Jul. 2015.

[132] C. Zenger, J. Zimmer, J.-F. Posielek, and C. Paar, "On-line entropy estimation for secure information reconciliation," in *Workshop on Wireless Communication Security at the Physical Layer*, Jul. 2015.

[133] J. Zhang and Y. Zheng, "Frequency-domain turbo equalization with soft successive interference cancellation for single carrier MIMO underwater acoustic communications," *IEEE Transactions on Wireless Communications*, vol. 10, no. 9, pp. 2872–2882, Sep. 2011.

[134] J. Zhang, Y. Zheng, and C. Xiao, "Frequency-domain equalization for single carrier MIMO underwater acoustic communications," in *Proc. of MTS/IEEE OCEANS Conf.*, Sep. 2008, pp. 1–6.

[135] J. Zhang, A. Marshall, R. Woods, and T. Duong, "Secure key generation from OFDM subcarriers' channel responses," in *Proc. of Globecom Workshops*, Dec. 2014, pp. 1302–1307.

[136] Y. Zhang, Y. Huang, L. Wan, S. Zhou, X. Shen, and H. Wang, "Adaptive ofdma for downlink underwater acoustic communications," in *Proc. of MTS/IEEE OCEANS Conf.*, Sep. 2014, pp. 1–5.

[137] ——, "Adaptive OFDMA with partial CSI feedback for underwater acoustic communications," *Journal of Communications and Networks*, Aug. 2015, (accepted).

[138] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[139] G. Zheng, I. Krikidis, C. Masouros, S. Timotheou, D.-A. Toumpakaris, and Z. Ding, "Rethinking the role of interference in wireless networks," *IEEE Communications Magazine*, vol. 52, no. 11, pp. 152–158, 2014.

[140] S. Zhou and Z. Wang, *OFDM for Underwater Acoustic Communications*. John Wiley & Sons, 2014.

[141] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, Nov. 2013.

[142] Y. Zhu, X. Lu, L. Pu, Y. Su, R. Martin, M. Zuba, Z. Peng, and J.-H. Cui, "AquaSim: An NS-2 Based Simulator for Underwater Sensor Networks," in *Proceedings of ACM WUWNet*, 2013.

[143] Y. Zhu, L. Pu, Z. Wang, X. Lu, R. Martin, Y. Luo, Z. Peng, and J.-H. Cui, "Underwater acoustic network protocol stacks: Simulator-based vs. OS-based," in *Proceedings of IEEE Oceans-St. John's*, 2014, pp. 1–7.