University of Southampton

Faculty of Engineering and Physical Sciences
Electronics and Computer Science

Resilient Communications for Tactical Systems

by

Alexander J. B. Hamilton
BEng, MSc, CEng, FIET, SMIEEE
ORCiD: 0000-0003-0604-6563

A thesis for the degree of
Doctor of Philosophy

February 2024

University of Southampton

Abstract

Faculty of Engineering and Physical Sciences
Electronics and Computer Science

Doctor of Philosophy

Resilient Communications for Tactical Systems

by Alexander J. B. Hamilton

In the rapidly evolving landscape of digital communications that defines our contemporary world, the imperative for resilient, secure, and distributed wireless systems has never been more crucial. Within the specific context of defence and security operations, the critical role of resilient, secure, and distributed wireless communications in fostering optimal situational awareness and facilitating information exchange cannot be overstated.

This thesis introduces innovative novel approaches and solutions to address the intricate technical challenges inherent in tactical communications. These challenges are particularly pronounced in scenarios such as urban deployments or underwater acoustic communications. The diverse techniques presented in this work include a pioneering Joint Source Channel Coding scheme, a novel Log Likelihood Ratio (LLR)-based signal processing demodulation technique for M-ary Orthogonal Signalling, novel turbo-equalization techniques tailored to a NATO standard, integrated security within a high-performance physical layer for underwater communications, and pioneering approaches to the integration of communications and autonomy. These advancements ensure optimal resource utilisation while minimising environmental and operational impact.

The robustness of several of the proposed solutions is evaluated through analysis and implementations in relevant scenario simulations. Real-world applicability and performance metrics are considered to validate the efficacy of the methodologies developed and their ultimate integration within existing defence and security frameworks.

Contents

List of Figures

Declaration of Authorship

I declare that this thesis and the work presented in it is my own and has been generated by me as the result of my own original research.

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published work of others, this is always clearly attributed;
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. Parts of this work have been published as: [1; 2; 3; 4; 5; 6; 7; 8]

Signed:..... Date:.....

Acknowledgements

Thanks to my supervisors, Rob and Mohammed, for supporting me in the pursuit of this research; it has not been easy, nor simple, but it has been a rewarding process.

Thanks also to my family, who have supported me through these times, in particular to Roeena who has put up with many long evenings and weekends where I have given up time I could have spent with our young family, also to our son Henry, and our dog Molly who always keep us on our toes and put a smile on our faces.

To all those in Nokia, UK Government, QinetiQ and the wider communications, defence and security community as well as other collaborators, both in the UK and Internationally, who are too many to mention, I thank you for the efforts and support.

Acronyms

E_b/N_0 Energy per Bit per Noise Power Spectral Density. 4, 7, 40

3GPP Third Generation Project Partnership. xxv, 37, 125, 148, 151, 153

AComP Allied Communication Protocol. 87, 100

AES Advanced Encryption Standard. 125, 127, 129, 130, 146

ANEP Allied Naval Engineering Publication. 140, 144

ASW Anti Submarine Warfare. 107–109, 136

AUV Autonomous Underwater Vehicle. xi, 107–110, 132, 135, 136

AWGN Additative White Gaussian Noise. 83

BCJR Bahl, Cocke, Jelinek, and Raviv. 59–61, 63, 91

BER Bit Error Rate. x, 91, 93, 94, 97–99

BFSK Binary Frequency Shift Keying. 24, 115, 140

BPSK Binary Phase Shift Keying. 24, 25, 77, 82

BT Bandwidth-Time. 77, 78, 118, 120, 123

BW Bandwidth. 118

CC Convolutional Code. x, 7, 39, 40, 67–72, 99

CCA Cognitive Communications Architecture. 137

CCMC Continuous Input Continuous Output Memoryless Channel. ix, x, 6, 49, 65–69, 71, 73, 87, 93, 100, 148

CDMA Code Division Multiple Access. 82

CMRE Centre for Maritime Research and Experimentation. 137, 142, 143

CND Check Node Decoder. 35, 36

CP-OFDM Cyclic Prefix - Orthogonal Frequency Division Multiplexed. 89, 90

CPM Continuous Phase Modulation. x, 87–91, 100, 148, 150

CRC Cyclic Redundancy Check. xi, 120, 130, 131

DCMC Discrete Input Continuous Output Memoryless Channel. 26, 148, 149

DSSS Direct Sequence Spread Spectrum. 77–79, 114, 117–121

Dstl Defence Science and Technology Laboratory. 7, 76, 151

EDA European Defence Agency. 139

EGEC Elias Gamma Error Correction. 43

EXIT Extrinsic Information Transfer. ix, x, 4, 7, 34–37, 41, 44, 49, 61, 63–68, 73, 95–98, 100, 101

ExpG Exponential Golomb. x, 7, 39, 40, 67–72

ExpGEC Exponential Golomb Error Correction. 43

FB-TE Full Block Turbo Equalizer. x, 93, 94, 96–100

FEC Forward Error Correction. 91

FH Frequency Hopping. 140

FLC Fixed Length Code. 45–48, 50, 53–56, 63

GCM Galois Counter Mode. 127, 129, 130

GPS Global Positioning System. xi, 108

HARQ Hybrid Automatic Repeat Request. 121

HDR High Data Rate. 121

IP Internet Protocol. 14, 26, 29, 152

ISI Inter Symbol Interference. 77, 78

IV Initialisation Vector. xi, 127, 128, 130, 131

JSCC Joint Source Channel Code. 4, 7, 39, 40, 42–44, 54, 61, 63, 66, 67, 69, 72, 73

LDPC Low Density Parity Check. ix, 20, 35, 36, 41, 43, 85

LFSR Linear Feedback Shift Register. 125

LLR Log Likelihood Ratio. iii, x, 4–6, 8, 32–35, 40, 59–62, 64, 65, 73, 75, 76, 79, 82–87, 91, 93, 95, 96, 119, 148, 150, 152

LTE Long Term Evolution. x, 91, 92

MCM Mine Counter Measures. xi, 108, 109

MF Medium Frequency. 110

MOS M-ary Orthgonal Signalling. 114, 117–121

MS Modulation Switch. xi, 123, 124

NATO North Atlantic Treaty Organization. i, iii, xxv, 3, 5, 9, 23, 37, 75, 87, 88, 92, 96, 100, 105, 106, 110, 126, 139, 140, 142, 144–146, 150, 151, 153

NBWF Narrowband Waveform. 23, 87, 88, 92, 93, 96, 100

NIAG NATO Industry Advisory Group. 144

OSI Open Systems Interconnection. xi, 29, 136–138

PAPR Peak to Average Power Ratio. x, 89, 90

PCIS Phorcys Cryptographic Interoperability Specification. 119, 128, 129

PN Pseudo Noise. 79

POMLS Phorcys Open Media Layer Specification. 121

PSK Phase Shift Keying. 117–121

QAM Quadrature Amplitude Modulation. 25, 89, 91

QPSK Quadrature Phase Shift Keying. x, 4, 6, 7, 39, 40, 44, 61, 62, 64–73, 88, 91, 115, 148–150, 152

REGEC Reordered Elias Gamma Error Correction Code. 7, 39, 40, 43, 44, 61, 66, 67, 69, 72, 73

RExpG Reordered Exponential Golomb. ix, 44–52, 54–57, 59, 61, 62

RExpGEC Reordered Exponential Golomb Error Correction. ix, x, 4, 6, 7, 39–45, 49, 50, 53–73, 148–150, 152

RF Radio Frequency. 77, 78, 132

SB-TE Sub Block Turbo Equalizer. x, 93, 94, 96–100, 150, 153

SHA Secure Hash Algorithm. 125

SISO Soft Input Soft Output. 91, 95

SNR Signal to Noise Ratio. ix–xi, 4, 7, 24, 40, 65–69, 72, 83, 85, 86, 92, 96–99, 112, 113, 153

SSCC Separate Source Channel Code. 4, 7, 39, 41–44, 61, 63, 67, 69, 72, 73

STANAG Standardization Agreement. 87, 88, 139, 140, 143–145

SWAP Size Weight and Power. 89, 91

TUBCipher Tiny Underwater Block Cipher. xi, 130, 131

UEC Unary Error Correction. 43, 55

UHF Ultra High Frequency. 87, 91, 92

URC Unity Rate Code. ix, x, 4, 6, 7, 39–41, 44, 61–73, 148–150, 152

USV Unmanned Surface Vehicle. xi, 108, 109

VHF Very High Frequency. 87, 91

VLF Very Low Frequency. 23, 87

VND Variable Node Decoder. 35

Published Works

During the course of this thesis there have been several items published 6 journal papers (3 as main author), 14 conference papers (4 as main author), and 80 standards contributions (all as main author). These are detailed as follows:

As Primary Author (Journal and Conference Papers)

Hamilton, Alexander, "EXIT Chart Analysis of the UMTS Turbo Code in VLF Channels," in *International Zurich Seminar on Communications-Proceedings*, ETH-Zürich, 2016 [9]

Hamilton, Alexander, S. Holdcroft, D. Fenucci, P. Mitchell, N. Morozs, A. Munafò, and J. Sitbon, "Adaptable Underwater Networks: The Relation between Autonomy and Communications," *Remote Sensing*, vol. 12, no. 20, p. 3290, 2020 [1]

Hamilton, Alexander, J. Barnett, A.-M. Hobbs, K. Pelekanakis, R. Petroccia, I. Nissen, and D. Galsdorf, "Towards Secure and Interoperable Underwater Acoustic Communications: Current Activities in NATO IST-174 Research Task Group," *Procedia Computer Science*, vol. 205, pp. 167–178, 2022 [2]

Hamilton, Alexander, J. Barnett, and A.-M. Hobbs, "Phorcys, an evolution of JANUS," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022 [3]

Hamilton, Alexander, P. Agard, F. Paris, B. Bertenyi, K. Spruyt, K. Murphy, and D. Peterson, "Standards-Based Agile Radio Systems and Tactical Interoperability; the use of 3GPP protocols in tactical networks," tech. rep., EasyChair, 2023 [10]

Hamilton, Alexander, M. El-Hajjar, and R. G. Maunder, "Reordered Exponential Golomb Error Correction Code for Universal Near-Capacity Joint Source-Channel Coding," *IEEE Access*, 2023 [4]

As Primary Author (Standards Contributions)

At RAN4 106, Athens, Greece, February 2023: [11][12][13]

At RAN4 106-bis-e, Online, March 2023: [14][15][16][17]

At RAN4 107, Incheon, Korea, April 2023:
[18][19][20][21][22][23][24][25][26][27][28][29][30]

At RAN4 108, Toulouse, France, August 2023:
[31][32][33][34][35][36][37][38][39][40][41][42][43][44][45][46][47][48]

At RAN4 108-bis, Xiamen, China, October 2023:
[49][50][51][52][53][54][55][56][57][58][59][60][61][62][63][64][65][66][67][68][69][70][71]

At RAN4 109, Chicago, USA, November 2023:
[72][73][74][75][76][77][78][79][80][81][82][83][84][85][86][87][88][89][90][91]

As 'Other' Author

A. Pérez-Pascual, **Hamilton, Alexander**, R. G. Maunder, and L. Hanzo, "Conceiving Extrinsic Information Transfer Charts for Stochastic Low-Density Parity-Check Decoders," *IEEE Access*, vol. 6, pp. 55741–55753, 2018 [92]

M. Zheng, **Hamilton, Alexander**, and C. Ling, "Covert Communications with a Full-Duplex Receiver in Non-Coherent Rayleigh Fading," *IEEE Transactions on Communications*, 2020 [93]

Y. Livran, V. Le Nir, S. Couturier, M. Suchanski, P. Kaniewski, J. Romanik, **Hamilton, Alexander**, P. Howland, and M. D. Tracy, "Electromagnetic environment situational awareness," in *2021 International Conference on Military Communication and Information Systems (ICMCIS)*, pp. 1–8, IEEE, 2021 [94]

E. Guler, C. Geldard, **Hamilton, Alexander**, and W. Popoola, "Subcarrier intensity modulation for turbulent underwater optical wireless communications," in *2021 Conference on Lasers and Electro-Optics (CLEO)*, pp. 1–2, IEEE, 2021 [95]

W. O. Popoola, C. Geldard, E. Guler, and **Hamilton, Alexander**, "Underwater optical wireless communication with subcarrier intensity modulation: an experimental demonstration," in *Proceedings of Meetings on Acoustics*, vol. 44, AIP Publishing, 2021 [96]

N. Morozs, P. Mitchell, D. Grace, T. Tozer, T. Bauge, and **Hamilton, Alexander**, "Phorcys Networking," *UCOMMS-22*, 2022 [97]

C. T. Geldard, E. Guler, **Hamilton, Alexander**, and W. O. Popoola, "An empirical comparison of modulation schemes in turbulent underwater optical wireless communications," *Journal of Lightwave Technology*, vol. 40, no. 7, pp. 2000–2007, 2022 [98]

A.-M. Hobbs, J. Barnett, and **Hamilton, Alexander**, "PCIS-A Novel Approach to Security in the UW Domain," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022 [5]

J. Davies, P. Randall, J. Neasham, B. Sherlock, and **Hamilton, Alexander**, "Phorcys Waveform Architecture," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022 [6]

J. Neasham, T. Corner, J. Davies, and **Hamilton, Alexander**, "Sea Trial Results and Receiver Performance Analysis for Phorcys V0 Waveform," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–5, IEEE, 2022 [7]

J. Chen, C. T. Geldard, E. Guler, **Hamilton, Alexander**, and W. O. Popoola, "An Experimental Demonstration of FSK-SIM-PDM Underwater Optical Wireless Communications," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022 [99]

J. Kellett, **Hamilton, Alexander**, J. Williams, and C. H. Wong, "Sub-Block Turbo Equalization for CPM Waveforms in Multipath Environments," in *2023 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–6, IEEE, 2023 [8]

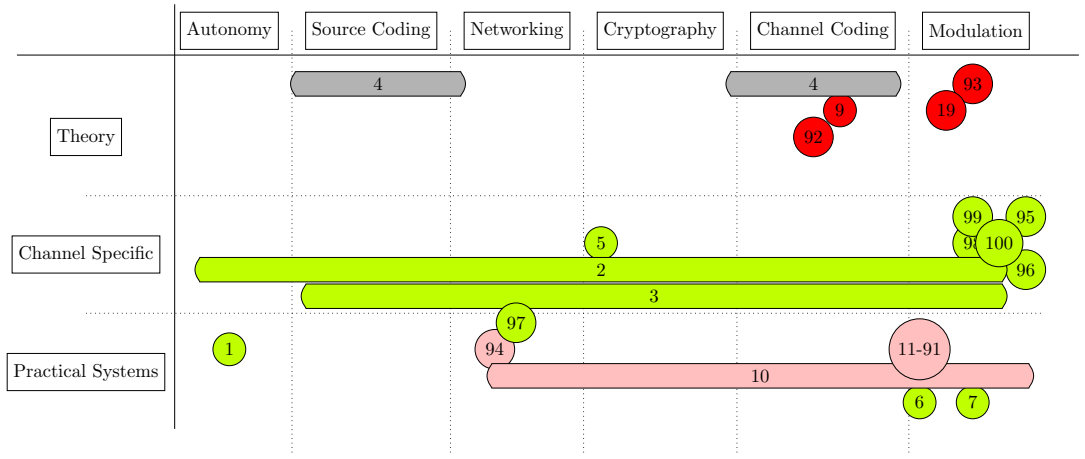
C. T. Geldard, E. Guler, I. M. Butler, **Hamilton, Alexander**, and W. O. Popoola, "Exploiting polarisation state for beyond 10 Gbps underwater optical wireless data transmission in hostile channel conditions," in *Next-Generation Optical Communication: Components, Sub-Systems, and Systems XII*, vol. 12429, pp. 172–175, SPIE, 2023 [100]

Preface

Throughout the PhD journey, the author has held various professional roles within the defence industry, the UK government, and the mobile telecommunications industry as a 3GPP standards delegate for Nokia. These positions have encompassed research lead responsibilities for the UK Ministry of Defence and NATO, and more recently within 3GPP.

Hence, the author has a large publication record, along with a track record of contributions and leadership within the wireless communications community. These contributions demonstrate the breadth of the author's research expertise in specific areas and highlight their knowledge and leadership across a range of subjects within the field.

In the figure below, we show the grouping of published material through the course of this thesis, where the groupings refer directly to the chapters of this thesis.



Scope of Published Work

The sections in gray are discussed in Chapter 3, those in red in Chapter 4, those in lime in Chapter 5, and those in pink are standards contributions which will not be discussed within this thesis.

As can be observed within the figure, the published work represents a breadth and depth of work ranging from autonomy, source coding, networking, cryptography, channel coding, and modulation. While this represents the published work of the author, the thesis itself will focus on research efforts specifically around source coding, channel coding, and modulation, as will be discussed in chapter 1.

Alongside these publications, the author has led and contributed to several efforts within the UK engineering community, including:

- Industrial Advisory Board, (2021-Current), Newcastle University, School of Electronic and Electrical Engineering
- Secretary (2018–2020), Treasurer (2020–2022), and Vice-Chair (2022—Current) IEEE UK and Republic of Ireland Information Theory Chapter

The author has also created and led the following communities, demonstrating a significant depth to their contributions to the field of wireless communications:

- UK Underwater Communications CETO community
- UK Defence Wireless Communications Symposium
- NATO Task Group — Secure Underwater Communications for Heterogeneous Systems
- NATO Task Group — Wireless Communications Standardisation Project

As can be seen, the author has provided major contributions throughout the course of the PhD to the body of knowledge and community in wireless communications; this has been developed through a series of research activities, not all of which are directly linked to the MPhil/PhD process at the University of Southampton but are the author's individual effort.

Chapter 1 : Introduction

In the realm of contemporary defence and security operations, the pivotal role of resilient, secure, and distributed wireless communications in fostering situational awareness and facilitating information exchange cannot be overstated, this is highlighted in the NATO Emerging and Disruptive Technology report [101], where communications are identified as a key disruptive technology area. As technological landscapes evolve, the demand for enhanced energy-efficiency, resilience, and robustness in wireless communication systems becomes increasingly critical, particularly within the dynamic and distributed contexts of tactical environments as evidenced by the recent increase in funding in the UK Government spending review in 2020 [102].

Against this backdrop, this thesis endeavours to address this imperative need by developing novel technology to augment the performance of wireless communication systems in distributed tactical settings. The thesis covers work in the field of information theory, source coding, channel coding, modulation, and autonomy to optimise energy-efficiency of tactical communications, ensuring judicious use of resources while concurrently addressing environmental concerns. The efficacy of the proposed solutions is evaluated through simulations and discussions on practical implementations in relevant scenarios.

This introductory chapter lays the foundation for a comprehensive exploration into wireless communications in distributed tactical environments. The subsequent chapters will delve deeper into the specific challenges, methodologies, and outcomes of the research, with the overarching goal of contributing to the advancement of energy-efficient, resilient, and robust wireless communication systems which are crucial for the success of defence and security operations.

1.1 Thesis Structure

The thesis is structured in a manner according to figure 1.1.1, whereby the thesis structure can be observed to align with a communications systems block diagram; focusing on source coding, channel coding, and modulation.

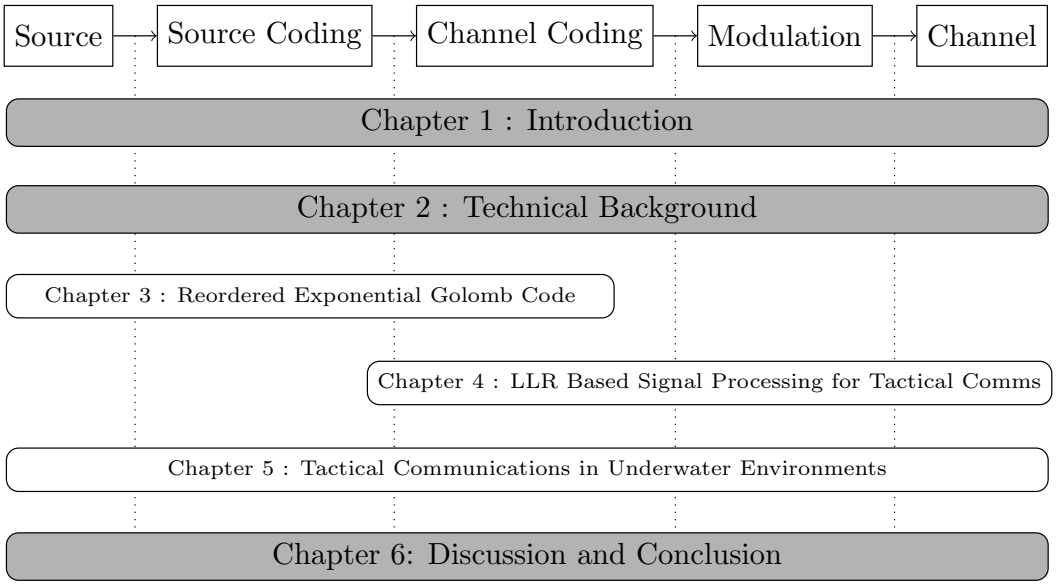


FIGURE 1.1.1: Structure of the Thesis

In Chapter 1, the reader is provided with an introduction and motivation for the thesis.

Chapter 2 provides some relevant background technical knowledge on source coding, channel coding, security, and information theory to aid in the reader's comprehension of further chapters within this thesis.

Chapter 3 introduces a novel Reordered Exponential Golomb Error Correction (RExpGEC) coding scheme [4], which is a Joint Source Channel Code (JSCC) technique designed for flexible and practical near-capacity performance. The proposed RExpGEC encoder and decoder are presented, and its performance is analysed using Extrinsic Information Transfer (EXIT) charts [103]. The flexibility of the RExpGEC is shown via the novel trellis encoder and decoder design. Finally, the Symbol Error Rate performance of the RExpGEC code is compared when integrated into the novel RExpGEC-Unity Rate Code (URC)-Quadrature Phase Shift Keying (QPSK) scheme against other comparable JSCC and Separate Source Channel Code (SSCC) benchmarkers. The RExpGEC-URC-QPSK scheme consistently operates within 2.5 dB of channel capacity when measuring E_b/N_0, whilst providing flexibility in SNR performance when compared to comparable benchmarkers. This novel scheme could be employed in tactical environments with limited bandwidth and constrained link budgets where capacity achieving code design is of utmost importance, for example, in underwater communication systems or land tactical communication systems.

Chapter 4 focuses on LLR based signal processing in tactical communications and introduces a novel bit-level LLR demodulation scheme for spread spectrum M-ary orthogonal signalling communications, such as those that may be used for underwater

acoustic communication or low power tactical communications schemes. The introduction of the bit-level LLR demodulation approach enables enhanced options for architecture in these schemes, which until now have only been able to use hard-decision bit-level values of symbol level channel coding schemes. Chapter 4 also introduces a novel turbo-equalizer for a continuous phase modulation scheme [8] and demonstrates the performance of this using the NATO Narrowband Waveform [104], ultimately to enable high-performance interoperability for NATO tactical ground units in a contested and congested environment, specifically showing performance within 1.1 dB of channel capacity. The novel turbo-equalizer demonstrates performance gains in realistic deployment scenarios, showing benefit over traditional block equalization techniques.

Chapter 5 focuses on underwater communications and introduces a novel communications protocol stack with integrated security and a high-performance physical layer [3] to cope with highly dispersive channels. This novel protocol stack includes a high-performance flexible physical layer design with integrated security, thereby enabling high-performance communications networks for submersible assets to protect the maritime interests of NATO nations.

The thesis concludes with a discussion of possible future research directions and a summary of the contributions contained within the thesis in Chapter 6.

1.2 Technical Areas of Thesis

While each chapter of the thesis provides the reader with insight into either the requisite technical background or novel contributions presented, the thesis itself can be broadly broken down into a subset of technical areas, as also shown in figure 1.1.1. These areas are as follows.

- Source Coding
- Channel Coding
- Modulation

These sections will be revisited in Chapter 6, when the thesis is drawn to a close, and are briefly outlined below.

1.2.1 Source Coding

Within the thesis, source coding is explored in both Chapter 2 and Chapter 3, where different approaches to source coding are reviewed and assessed against different source

distributions. Specifically, within Chapter 3, a novel source coding scheme is proposed within the novel RExpGEC joint source-channel code.

1.2.2 Channel Coding

Further to the activities on source coding, the thesis also introduces novel Channel Coding techniques in Channel 2, with the primary focus within Chapter 3. The novel RExpGEC scheme, when combined with the URC (and QPSK modulation), becomes the novel RExpGEC-URC-QPSK communications scheme, which consistently operates within 2.5 dB of channel capacity for any given source distribution. Within Chapter 5, channel coding is also further explored, albeit briefly within the Phorcys communications scheme.

1.2.3 Modulation

Modulation, or more specifically novel demodulation and equalization schemes, is another feature explored within this thesis.

Aspects of demodulation are discussed in chapters 2, 4, and 5. In Chapter 4, a novel bit-level LLR demodulation approach for M-ary Orthogonal signalling is introduced, as is a novel turbo equalization approach for differentially encoded modulation in challenging phase inversion environments, which shows benefits in relevant operational deployments and performance within 1.1 dB of the Continuous Input Continuous Output Memoryless Channel (CCMC) capacity bound.

Within Chapter 5, the same techniques introduced in Chapter 4 can be exploited within the novel Phorcys protocol suite to enable enhanced performance of tactical communications in various environments, whereby the protocols have been tested in several operational scenarios in [7; 2].

1.3 Thesis Contributions

As outlined in the preface of the thesis, the author has a substantial publication record, demonstrating their novel contributions to the wireless communications community. However, not all of these publications are directly pertinent to the thesis. Therefore, select publications are featured here, specifically emphasising their novel material and contributions to each relevant chapter.

1.3.1 Contributions of Chapter 3

Chapter 3 has significant contributions from the following publication:

Hamilton, Alexander, M. El-Hajjar, and R. G. Maunder, "Reordered Exponential Golomb Error Correction Code for Universal Near-Capacity Joint Source-Channel Coding," *IEEE Access*, 2023

Chapter 3 and the above publication introduce the novel RExpGEC coding scheme, a flexible and practical JSCC technique aimed at achieving near-capacity performance. We present the RExpGEC encoder and decoder, analysing its performance through EXIT charts [105]. The scheme's flexibility is demonstrated with a novel trellis encoder and decoder design.

We compare the symbol error rate performance of the RExpGEC code when integrated into the RExpGEC-URC-QPSK scheme against comparable JSCC and SSCC benchmarks. Specifically, the RExpGEC-URC-QPSK scheme is compared with the REGEC-URC-QPSK scheme [106] and a serial concatenation of Exponential Golomb (ExpG) [107] and Convolutional Code (CC) [108], forming the ExpG-CC-URC-QPSK scheme. Simulation results highlight the superior performance and flexibility of the RExpGEC-URC-QPSK scheme in providing reliable and efficient communications.

In an uncorrelated Rayleigh fading channel, the RExpGEC-URC-QPSK scheme outperforms SSCC by 2 to 3.6 dB (dependent on source distribution). Additionally, it consistently operates within 2.5 dB of channel capacity when measuring E_b/N_0, offering flexibility in SNR performance compared to the REGEC-URC-QPSK scheme. However, these performance gains come at the cost of complexity, with the RExpGEC-URC-QPSK scheme being 3.6 times more complex than the ExpG-CC-URC-QPSK scheme under certain conditions.

1.3.2 Contributions of Chapter 4

Chapter 4 has contributions from the following publication:

J. Kellett, **Hamilton, Alexander**, J. Williams, and C. H. Wong, "Sub-Block Turbo Equalization for CPM Waveforms in Multipath Environments," in *2023 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–6, IEEE, 2023[1]

[1]Chapter 4 exclusively encapsulates the contributions of the author of this thesis. It is crucial to highlight that the author served as the lead researcher for the published paper. However, owing to the timing of the paper's publication after their tenure at Dstl, Joe Kellett, who was employed with Defence Science and Technology Laboratory (Dstl) at the time of publication, assumed the role of the primary author for submission, in accordance with the requirements of the publication processes within the UK government.

Chapter 4 introduces novel techniques that enable the generation of bit-level LLR within M-ary orthogonal signalling, enabling flexible soft decoding of bit-level channel coding schemes, which in contrast to current methods [109] which compromise performance by relying on hard-decision approaches to obtain bit-level values, potentially enhancing performance by 2 or 3dB as well as enable greater flexibility of channel coding scheme. Additionally, the chapter emphasises a novel equalisation approach specifically tailored for challenging environments, customised for differentially encoded modulation schemes. The efficacy of this scheme is evaluated in Rayleigh fading channels [110], simulating tactical urban deployment scenarios [111]. The assessment reveals noteworthy improvements, especially in scenarios characterised by rapid phase inversions, such as those encountered by helicopters in deployment scenarios where traditional equalizers [112] may falter, and fail to converge (as is shown in simulation results in Chapter 4). The aspects relating to the novel turbo-equalizer were published in the above paper.

1.3.3 Contributions of Chapter 5

Chapter 5 has significant contributions from the following publications:

Hamilton, Alexander, J. Barnett, A.-M. Hobbs, K. Pelekanakis, R. Petroccia, I. Nissen, and D. Galsdorf, "Towards Secure and Interoperable Underwater Acoustic Communications: Current Activities in NATO IST-174 Research Task Group," *Procedia Computer Science*, vol. 205, pp. 167–178, 2022

Hamilton, Alexander, J. Barnett, and A.-M. Hobbs, "Phorcys, an evolution of JANUS," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022

Hamilton, Alexander, S. Holdcroft, D. Fenucci, P. Mitchell, N. Morozs, A. Munafò, and J. Sitbon, "Adaptable Underwater Networks: The Relation between Autonomy and Communications," *Remote Sensing*, vol. 12, no. 20, p. 3290, 2020

Chapter 5 also draws upon aspects of the following publications[2]:

J. Neasham, T. Corner, J. Davies, and **Hamilton, Alexander**, "Sea Trial Results and Receiver Performance Analysis for Phorcys V0 Waveform," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–5, IEEE, 2022

J. Davies, P. Randall, J. Neasham, B. Sherlock, and **Hamilton, Alexander**, "Phorcys Waveform Architecture," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022

[2]Contributions from the following papers exclusively represent the work of the author of this thesis, unless explicitly mentioned within the respective sections.

A.-M. Hobbs, J. Barnett, and **Hamilton, Alexander**, "PCIS-A Novel Approach to Security in the UW Domain," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022

N. Morozs, P. Mitchell, D. Grace, T. Tozer, T. Bauge, and **Hamilton, Alexander**, "Phorcys Networking," *UCOMMS-22*, 2022

Chapter 5 highlights the novel contributions the author has made to the field of underwater acoustic communications, specifically offering a departure from prior works that often focused narrowly on specific aspects or minimal viable products for interoperability [113; 114; 115; 116; 117; 118]. At the forefront of this chapter is the introduction of a novel, holistic communications protocol, Phorcys, which considers both performance and security aspects, to meet the needs of the operational community. The result is the Phorcys protocol suite [109], aspects of this have been published in [3; 7; 5; 97] as mentioned above.

Chapter 5 further showcases aspects of the standardisation efforts and how Phorcys sits within the context of NATO standardisation, in particular the NATO IST 174 Research Task Group, the novel contributions of the author (who chaired IST 174 from 2017 until 2023) which have been published in [2].

Furthermore, within Chapter 5, the reader is also presented novel approaches to how communications and autonomy can work together to achieve overall operational goals, this novel approach presented within Chapter 5 is also published in [1]. This is in direct contrast to the more common approach of simply communications being an enabler for autonomy.

Importantly, the content presented from these papers within this thesis stands as the exclusive work of the author.

Within Chapter 1, a brief introduction to the thesis has been provided, along with highlighting some areas which will be explored through the thesis itself.

In the following chapter, Chapter 2, the author will be provided with the requisite background knowledge to delve into the technical chapters of the thesis.

Chapter 2 : Technical Background

This chapter aims to provide the reader with a high level background introduction to some key concepts discussed through the thesis.

Core technical topics which are shared across Chapter 3, Chapter 4, and Chapter 5 are introduced within the chapter, with specific information background pertaining to the knowledge of each chapter contained within each chapter itself.

Chapter 2 can be seen within the structure of the overall thesis in figure 2.1.1.

This chapter covers the entirety of the technical aspects of the thesis, providing a background on source coding, channel coding, security and basic information theory aspects. It provides requisite knowledge to aid the reader in understanding further chapters of the thesis.

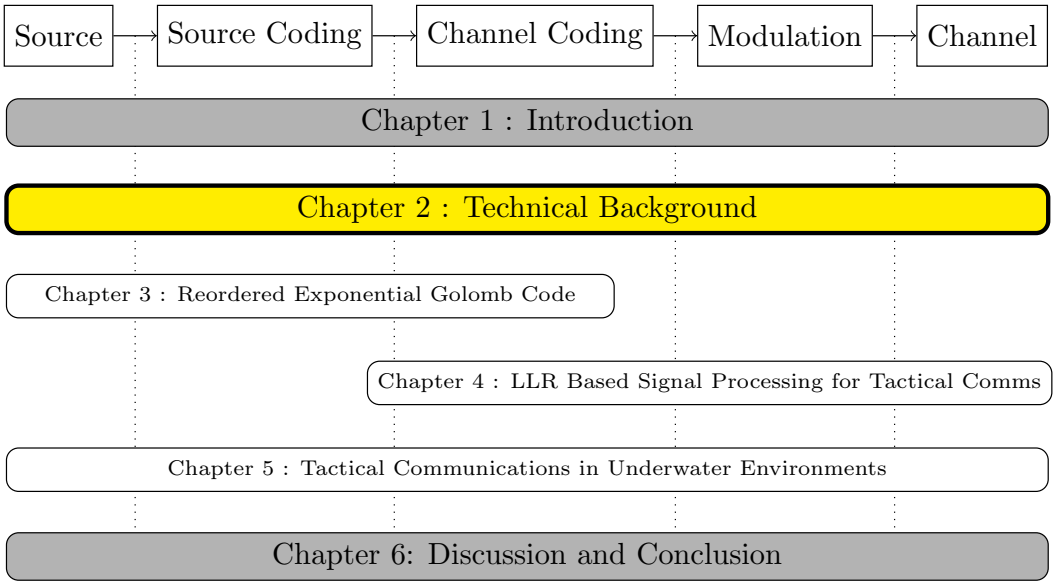


FIGURE 2.1.1: Structure of the Thesis

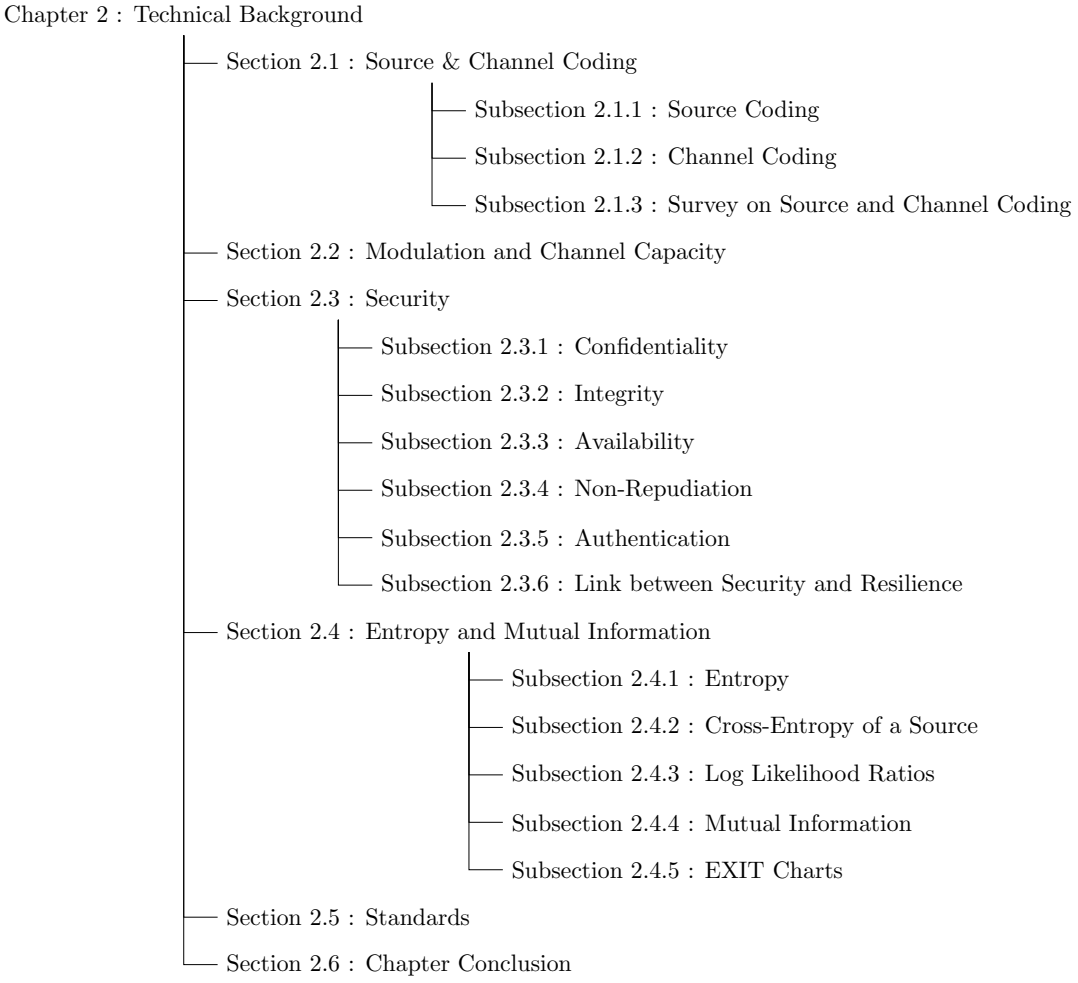


FIGURE 2.1.2: Structure of Chapter 2

It also frames the knowledge of the reader to understand the benefit that these approaches will provide to resilient tactical communications systems.

The chapter's organisation is evident in figure 2.1.2, illustrating the essential information covered within this section. As depicted in figure 2.1.1, this encompasses the entirety of the technical topics of the thesis.

2.1 Source and Channel Coding

Within this section, the reader is provided an introduction into the source and channel coding, whereby source coding [119; 120; 121; 122; 123] provides the data compression of a source to efficiently transmit symbols from an information source and then the channel coding [119; 124; 125; 126; 127; 128; 129; 130; 131] provides redundancy in order to robustly transmit this information over a noisy channel.

The optimal performance of source and channel coding can be defined by Shannon's separate source and channel coding theorem, originally proposed in [119] which establishes the limit for noiseless transmission of information, via means of providing separate source coding and channel coding.

In this seminal work, Shannon proposes and mathematically shows that there is a known limit to all communications, which is bound by the entropy of the information source[1] and then separately on how the communications protocol can cope with the noise of the channel, and define the channel capacity for a continuous input memoryless channel.

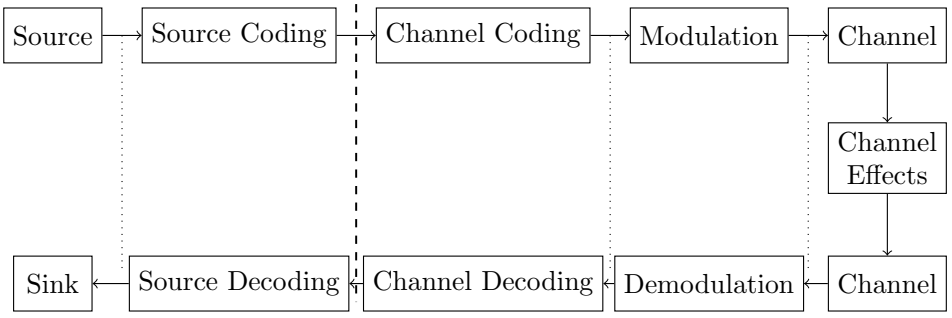


FIGURE 2.1.2: Block Diagram of a Communications System

In order for this to be realised in a discrete and noisy channel, the information content needs to be processed in a manner that both the transmitter and receiver are aware of [132; 123; 133]. This includes several distinct phases, which can be observed in figure 2.1.2.

Working back from the channel, we observe that information needs to be mapped to transmitted symbols, referred to as **modulation**[2]. These mapped symbols, as can be observed pictorially in the simple binary symmetric channel in figure 2.2.1 where the communications channel will exhibit some form of noise, which can be in the form of Gaussian noise or via a fading channel, or indeed many other means.

This noise causes errors in the transmitted symbols, therefore a communications scheme would wish to use some error correction, or more accurately **channel coding**, in order to enable error-free reception at the transmitter and recover corrupted symbols. The channel conditions in which error-free communications can be achieved, is therefore a function of the channel itself, the modulation scheme employed, and the channel coding used [124; 125; 126; 127; 128; 129; 130; 131].

[1] The concept of entropy in respect to information theory will be further expanded upon in Section 2.4.

[2] The term 'Modulation' [133; 134; 119] specifically refers to modulation of a carrier in a specific manner to infer the specific symbols; however, this will be further explored in Section 2.2.

Moving further back towards the information source, and past the boundary proposed by Shannon's separate source and channel coding theorem [119], we move to **source coding**. Source coding has several purposes; firstly it is a method of which information can be turned into a message that is understood by both transmitter and receiver, in the way that ASCII [135] can represent alphanumeric characters, that in turn can create stories to relay information. However, secondly source coding can be used to efficiently encode the information source as close as possible to its entropy limit, this will be further discussed in Section 2.1.1.

It is worth noting that there are various other aspects of a communications system that will not be described in detail in this thesis, including but not limited to; networking, synchronisation, channel access schemes and hardware design.

Security will be touched on lightly during the thesis, however not to the same depth as channel coding, source coding, or modulation as security is not one of the core areas of research for this thesis. However, the thesis proposes that security should not be considered as a separate cryptographic process, but instead embedded in communications systems design, this is discussed in Chapter 5. A brief introduction to some security aspects is provided in Section 2.3

2.1.1 Source Coding

Source coding is used to interpret the source efficiently, there are many types of source coding, ranging from those used for data compression, such as the LZW algorithm [136] all the way through to advanced video codecs used for streaming video on modern Internet Protocol (IP)-based video on-demand services, such as the H.265 video codec [137].

In the context of information theory, a source refers to the origin or producer of information [132]. It is the entity that generates a sequence of symbols or messages, and these symbols collectively form the output or data produced by the source. The concept of a source is fundamental to understanding information theory, as it helps in analysing and quantifying the information content within a given set of data.

Information sources can exhibit a wide range, encompassing simple processes like coin flips with binary outcomes (heads or tails) to more intricate sources such as natural language text [138] or digital images [139]. The nature of the source plays a pivotal role in determining the statistical properties and structure of the information it generates.

When discussing information distributions, we are delving into the likelihood or probability distribution [140] associated with the symbols or messages produced by the information source. In essence, the distribution articulates the probability of each potential outcome or symbol that the source can generate. A grasp of the information's

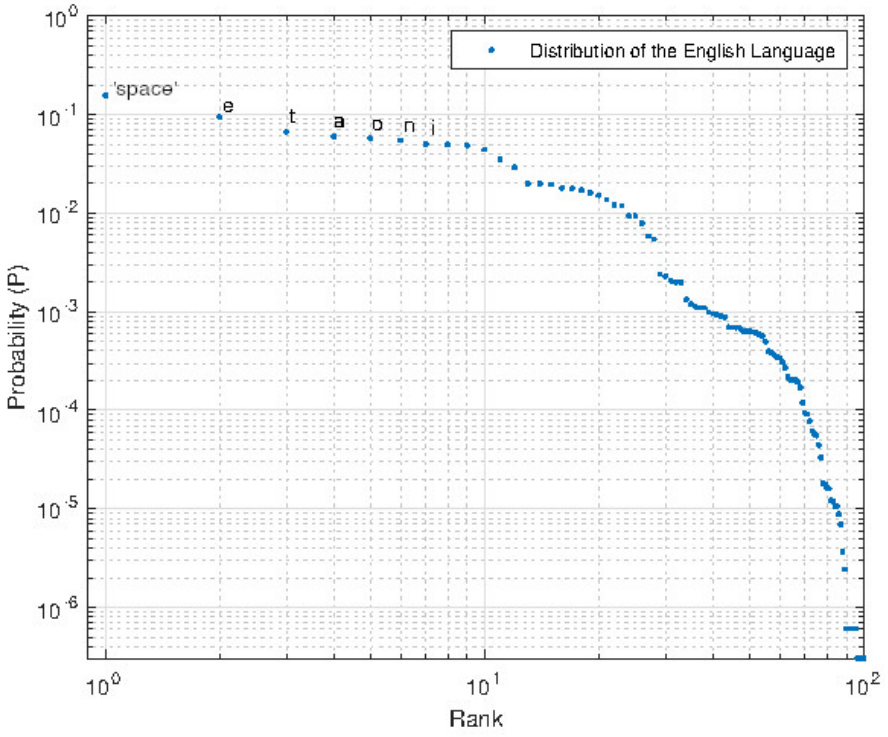


FIGURE 2.1.3: Source Distribution of the English Language

distribution facilitates the computation of metrics like entropy [119], providing a quantification of the average uncertainty associated with the outcomes of the source.

An information source can be characterised by its source distribution and the probability of each symbol occurring within a statistically significant set. A well-known example is the source distribution of the English Language, exemplified in figure 2.1.3, representing the distribution of English letters in the book "War and Peace" [138].

The work in this thesis focuses on various monotonical source distributions, based on geometric and zeta distributions. These distributions, which can be characterised by the probability of the symbol in rank 1, which can describe almost any source distribution with a good fit.

The Zeta distribution [141; 142], denoted by the Riemann Zeta function, is a discrete probability distribution employed to model symbol occurrences. Its probability function is expressed as $P(X = k) = \frac{1}{\zeta(s) \cdot k^s}$, where $s > 1$ represents the shape parameter, and $\zeta(s)$ is the Riemann Zeta function evaluated at s. In contrast, the Geometric distribution probability function [143] is given by $P(X = k) = (1 - p)^{k-1} \cdot p$, where k denotes the number of symbols, and p signifies the probability of each symbol. An example of a geometric source distribution would be the letters of the English alphabet, as shown in figure 2.1.3. To produce figure 2.1.3 the occurrence of each individual letter of the book "War and Peace" [138] were

calculated, and the probability plotted to understand the distribution these symbols produced, the reference text was deemed a large enough source to produce a valid distribution, and through analysis was representative of our source texts.

Source coding approaches and classes will be discussed in more detail in Chapter 3, as well as later in this chapter, whereby a survey into different source coding schemes is provided.

To provide an example to bring into frame the benefit achieved by source coding and the compression it can provide to a representative source, a brief worked example of a common source coding approach and a fundamental technique in information theory and data compression, the Huffman code [144] is presented below. It is important to note that the Huffman code is not suitable for infinite or huge information sources due to a requirement to maintain a known 'dictionary' at both transmitter and receiver for each distribution.

The basic idea behind Huffman coding [144] is to create a variable-length prefix code, where shorter codes are assigned to more probable symbols and longer codes to less probable symbols. This is achieved through a two-step process: frequency/probability analysis and tree construction.

1. Frequency/Probability Analysis
    - The first step involves analysing the input data to determine the frequency and probability of each symbol.
    - This information is used to build a frequency/probability table, listing each symbol and its corresponding frequency/probability in the input data.
2. Tree Construction
    - Using the frequency table, a binary tree called the Huffman tree is constructed. The construction process involves repeatedly combining the two least frequent symbols (or subtrees) into a new subtree until a single tree is formed.
    - During this process, a binary code is assigned to each symbol based on the path taken to reach it in the tree. Going left or right in the tree corresponds to appending a '0' or '1' to the code, respectively.

To provide an example of the Huffman code, a series of 'toy' symbols and representative probabilities are presented in Table 2.1.1. Including the representative symbol probabilities, output codewords (derived from the tree, which is later presented in figure 2.1.4), output codeword lengths and output averaged codeword length contribution (probability multiplied by codeword length).

TABLE 2.1.1: Example Huffman Code Parameters

Symbol	a	b	c	d	e
Probability	0.10	0.15	0.30	0.16	0.29
Codeword	010	011	11	00	10
Codeword Length	3	3	2	2	2
Average Codeword Length Contribution	0.30	0.45	0.60	0.32	0.58

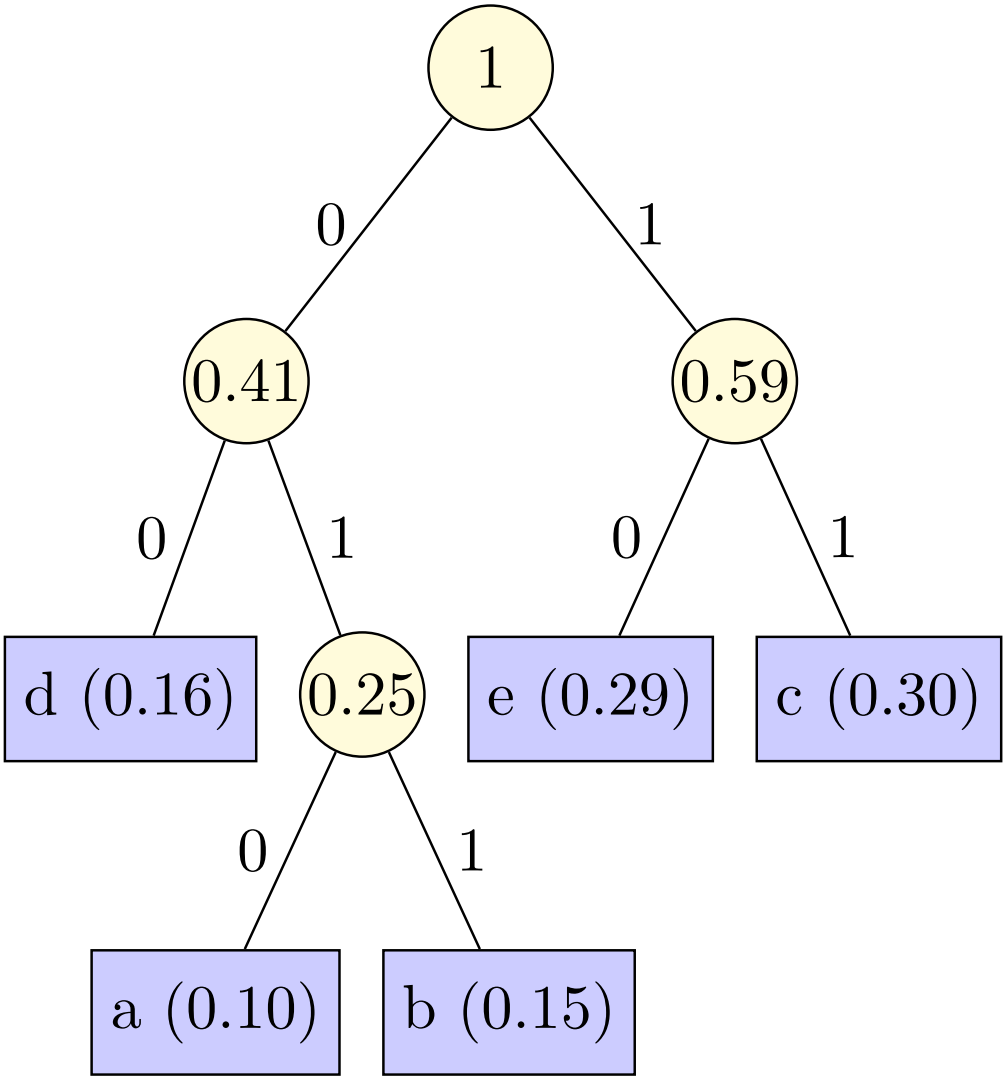


FIGURE 2.1.4: Example Huffman Tree

The corresponding Huffman tree from Table 2.1.1 is presented in figure 2.1.4. The mapping within this tree ensures that no code is a prefix of another, making the codes uniquely decodable. Due to the variable-length nature of Huffman codes, more frequent symbols are assigned shorter codes, leading to overall compression of the data.

To illustrate, we can encode the bit stream corresponding to the symbols a, e, c, e, c, d using the Huffman tree depicted in figure 2.1.4. In this scenario:

- Symbol a is encoded as $0, 1, 0$,
- Symbol e is encoded as $1, 0$,
- Symbol c is encoded as $1, 1$,
- Symbol d is encoded as $0, 0$.

Concatenating these encoded symbols together, the resulting bit stream is $0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0$, with a length of 13 bits. In contrast, if these symbols were transmitted in ASCII [135] (resulting in 8 bits per symbol), the total would be 48 bits. This signifies an efficiency saving of 370 percent in comparison to ASCII coding.

Huffman coding is widely employed in various applications to provide efficient transmission of data when a source is exactly known [133; 134]. The concerns of knowing the exact source information in practical deployment scenarios are discussed later in this chapter. In the case of the example shown above, the averaged codeword length becomes 2.25 bits (the sum of the values in row 5 of figure 2.1.4), which is less than the codeword length of 3 bits which would be applied if each symbol was provided a binary index. This efficiency in representing data with minimal redundancy makes it a key component in the field of data compression.

2.1.2 Channel Coding

To improve the performance of communications systems and to remove errors from noisy channels, it is required to provide some form of redundancy to the transmitted symbols in such a manner as to provide the receiver a method to infer what the intended transmission was. This redundancy is achieved through the use of coding mechanising, typically (but not always) applied to binary steams or blocks of data to cope with the channel effects, hence the term channel coding.

The simplest form of channel coding is a repetition code [145; 133; 146], whereby the input bits are simply repeated to form redundancy and combined at the decoder to provide more resilience in noisy channels.

A slightly more complex code that is one of the seminal channel coding techniques and widely used is the Hamming code, which was originally proposed in [147]. It is particularly effective in detecting and correcting single-bit errors within a block of data. The primary purpose of the Hamming code is to add redundancy to the transmitted information in such a way that errors can be identified and corrected.

The fundamental concept behind the Hamming code involves augmenting the original data with parity bits. Parity bits, additional bits appended to the data bits, have values determined based on the parity of corresponding sets of data bits. The most

prevalent manifestation of the Hamming code is the (7,4) code, which encodes 4 bits of data into a 7-bit code. The three additional bits function as parity bits, strategically positioned to confer error detection and correction capabilities. An illustrative example is provided below.

The (7,4) Hamming code can be defined by a series of equations. In the example presented in this section, these equations are represented as in Eq. (2.1) below, specifying how the Hamming code can be constructed.

$$\begin{aligned} P_1 &= D_1 \oplus D_2 \oplus D_3 \\ P_1 &= D_2 \oplus D_4 \\ P_1 &= D_2 \oplus D_3 \oplus D_4 \end{aligned} \tag{2.1}$$

These equations can also be represented as a Generator Matrix, which for the equations in Eq. (2.1) are represented in Eq. (2.2) whereby the input data vector (of 4 information bits) can be multiplied with the matrix G to generate an output Hamming codeword. The additions are performed modulo 2 to produce the binary output codeword.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{2.2}$$

Using the example generator matrix in Eq. (2.2), it is possible to encode the data bit stream $'0, 0, 0, 1'$. This encoding involves matrix multiplication modulo 2 with G, resulting in the output codeword $'0, 0, 0, 1, 0, 0, 1'$. As illustrated in this example, the first four bits are identical to the information bits, owing to the identity matrix comprising the initial four columns of G.

In practice, G is composed of an identity matrix with a length equal to that of the input codeword (m) and a parity check matrix of size (n $\times$ m), where n represents the parity length, and m denotes the input codeword length.

The Hamming code can be further represented in a 'Tanner Graph', as seen in figure 2.1.5 which is a bipartite graph illustrating the data bits and parity bits along with the 'edges' connecting them.

It is along these edges that a decoder architecture could utilise to identify an error in a codeword. By using these edges, the decoder can calculate the erroneous bit and correct it.

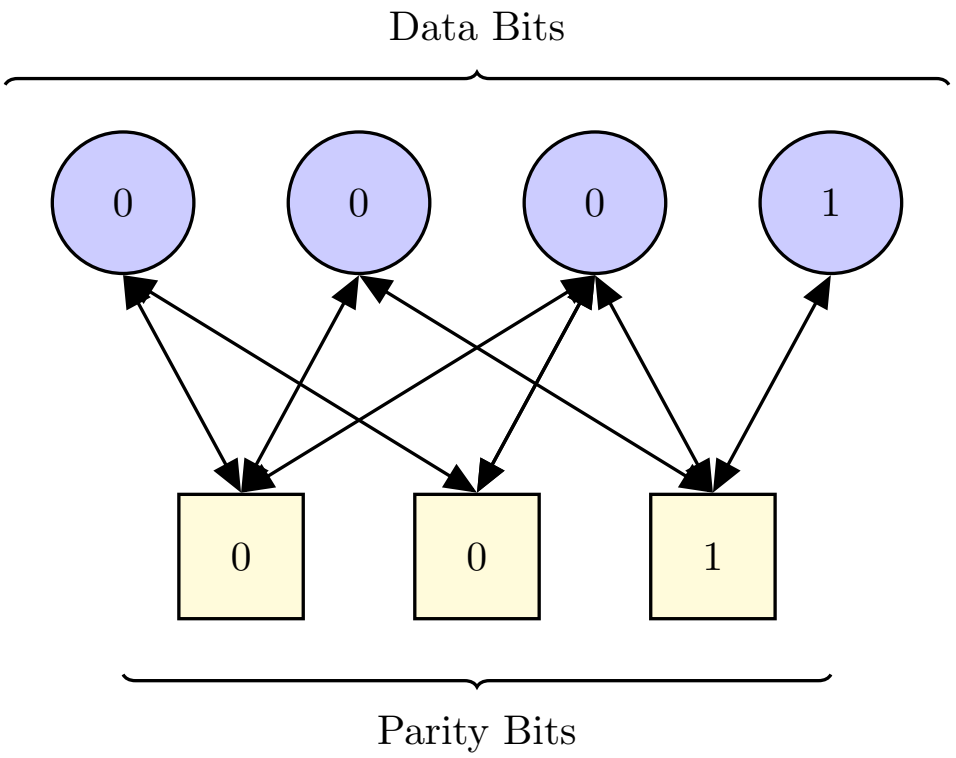


FIGURE 2.1.5: Hamming Code Tanner Graph

The Tanner graph constitutes a fundamental approach to understanding the inherently parallel architecture of the Low Density Parity Check (LDPC) code [125], which finds application in modern communication standards like 5G new radio [148]. In some respects, the LDPC can be viewed as an extension of the Hamming code. However, it employs an iterative approach with a considerably larger number of nodes, enabling it to achieve near-capacity communications. In this iterative decoding process, the variable nodes transmit information to the check nodes along the edges, and subsequently, the check nodes relay the information back to the variable nodes along the edges. This process continues until either a fixed number of iterations is complete, or the decoder is confident that it has converged upon the correctly transmitted codeword.

One potential method for the decoder to ascertain it has received the correct codeword is to perform a syndrome check [149; 126]. The term “syndrome” pertains to the set of values obtained by checking the parity of received bits against the expected parity. Specifically, the syndrome is a vector indicating whether errors are present in the received codeword and providing information about their locations.

Upon receiving a codeword, it is assessed against the parity check matrix of the LDPC or Hamming code. The syndrome is computed by multiplying the received codeword

by the transpose of the parity check matrix. If the received codeword is devoid of errors, the syndrome vector is zero, prompting the iterations to cease as the received codeword is deemed correct.

One key feature of the Hamming code is its ability to detect and correct single-bit errors. The parity bits are carefully positioned to cover specific combinations of data bits, allowing the receiver to identify and correct errors by comparing the received parity bits with the recalculated ones. However, the Hamming code has limitations, as it can only correct single-bit errors and detect some double-bit errors; many modern channel coding schemes have much greater ability to correct and decode larger bit errors, especially with longer block sizes, as can be seen in [124; 125; 126; 127; 128; 129; 130; 131].

2.1.3 Survey on Source Coding

To comprehend the most suitable source coding scheme for tactical communications, an extensive survey of the existing literature on source coding techniques was undertaken.

A total of 53 papers were reviewed, often encompassing several source coding schemes within each paper. This resulted in a comprehensive review of 84 source coding schemas, with a subset of these presented in Table 2.1.2.

The predominant focus of research in the source coding field has been propelled by either:

- Video codec and efficient compression
- Large volume file compression

These efforts are primarily motivated by the cost of data storage and the substantial data throughput requirements for video. Unfortunately, some prerequisites for tactical communications, especially in terms of voice, small file, and text transfer, do not align well with these objectives. Consequently, the relevance and applicability of these coding schemes to tactical communications will be discussed at pertinent junctures within the thesis.

Within the survey, two primary categories of source coding schemes emerge: dynamic and static. These categories can be broadly defined as follows.

TABLE 2.1.2: Survey of several source coding schemes

Contribution	Ref.	BPC	Year	Static/Dynamic	Family
Greedy	[120]	3.192	2002	Static	Grammar
Sequitur	[120]	2.881	2002	Static	Grammar
Large Neural Network	[121]	2.283	2000	Static	Neural Network
Small Neural Network	[121]	2.508	2000	Static	Neural Network
Back Propagation Neural Network	[150]	N/A	2008	Static	Neural Network
Arithmetic Coding and Predictor Network	[151]	3.636	1996	Static	Combination
Huffman Coding and Predictor Network	[151]	2.962	1996	Static	Combination
Minimal Euclidean Distance and Predictor Network	[151]	3.636	1996	Static	Combination
Huffman Coding	[151]	4.697	1996	Static	Combination
lz4	[152]	3.801	2022	Static	Combination
zstd	[153]	2.528	2023	Static	Combination
zlib	[154]	2.581	2023	Static	Combination
Lempel-Ziv Coding	[151]	3.940	1996	Dynamic	Combination
Exponential Golomb, k = 1	[142]	6.117	2016	Static	Unary
Exponential Golomb, k = 0	[142]	2.989	2016	Static	Unary
Modified Adaptive Huffman	[155]	3.03	2009	Static	Huffman
Adaptive Coding	[156]	2.192	1984	Dynamic	Combination
decomp8	[157]	1.276	2009	Combination	Prediction
paq8	[157]	1.394	2009	Combination	Prediction

- **Static source coding schemes:** Involve compression methods where the encoding process remains fixed and does not adapt dynamically to changing data patterns. In these schemes, the mapping of symbols to code words is predetermined and does not depend on the context or statistical properties of the source data.
- **Dynamic source coding schemes:** Represent an adaptive approach in information theory. These schemes adjust the encoding process based on evolving data patterns. Unlike static coding, dynamic coding responds to changes in the statistics or context of the source data. This adaptability allows the system to optimise compression efficiency in response to fluctuations in symbol frequencies.

These coding schemes can also be categorised into different families:

- **Grammar-Based source coding schemes:** Employ grammatical structures to represent and compress data. Instead of encoding individual symbols directly,

these schemes construct a grammar that describes the rules governing data generation, representing segments of the data through rules and references to the grammar.

- **Neural Network coding schemes:** Leverage the ability of neural networks to learn complex patterns and representations. Trained to encode and decode data efficiently, the encoding process maps input data into a compressed representation, and the decoding process reconstructs the original data from this compressed form.
- **Prediction coding schemes:** In information theory, involve encoding data based on predicted values rather than explicit representation, leveraging the concept that much of the information in a sequence can be inferred or predicted from its preceding elements.

The survey revealed that optimal coding schemes for data compression are often based on dynamic and dictionary-based encoding, where dynamic dictionaries adapt to the input source data [157]. However, these schemes are not directly applicable to wireless communications, where messages must adhere to a defined block size according to the wireless protocol stack in use.

For communication systems like common data link [158], NATO Narrowband Waveform [104], and Very Low Frequency communications [159], the block sizes are much shorter than those used to achieve compression ratios of $\tilde{1}.3$, as seen in [157] and [121]. Therefore, when selecting source coding schemes for wireless communications, it is essential to choose a scheme that aligns with an output block size corresponding to a length less than or equal to the minimum block size of that particular system.

Moreover, in systems constrained by a small block size, there is a desire to ensure minimal energy per bit is used considering the channel environment. In [119], it is demonstrated that reliable transmission is possible through optimal implementation of source and channel coding, but this holds true only if all transmitted bits contain information. Therefore, if padding is required to meet higher layer protocol requirements, it implies wasteful energy transmission.

To maximise the efficient transmission of information, **symbol-level or short dictionary-based schemes** are preferred for wireless protocols, where a system must decode all information within a block using only a single transmission of the block itself.

The efficiency rate can be defined as the length of the information bits as a proportion of all bits used in the transmission, including bits used to transit information, those used to pad up to a specific finite block length, those used for error correction, and those used in any header functionality. This is expressed in Eq. (2.3).

$$\textit{Efficiency Rate} = \frac{Length(bits_{information})}{Length(bits_{information} + bits_{padding} + bits_{error\,correction} + bits_{header})} \tag{2.3}$$

This therefore corresponds to an efficiency loss, shown in Eq. (2.4) of the overall transmitted message. Which can be translated to the expected loss in Energy per Information bit to noise power spectral density. It is important to note that the code rate and the SNR performance will be unaffected by the padding, as these parameters are independent of which of the a priori (to the channel code) bits are true information bits.

$$\textit{Efficiency Loss} = 10\ \log_{10}\left(Efficiency\,Rate\right) dB \tag{2.4}$$

2.2 Modulation and Channel Capacity

Modulation is the process of transferring information onto a medium, via the process of mapping transmission bits onto symbols which are then sent over a channel.

Modulation itself can be done in various ways, by manipulating the phase, amplitude, frequency, orbital momentum or any other parameter within which that medium can be manipulated to create symbols.

For traditional radio communications, and indeed acoustics, modulation is typically conducted via the means of phase, amplitude, and frequency manipulation; a communications scheme designer may choose to fix one or more of these parameters for various reasons, including hardware constraints. Therefore, via manipulation of these parameters, it is possible to create a series of distinct discrete symbols, for which, when given a specific channel, a probability can be calculated of correct transmission.

In figure 2.2.1 it is possible to observe a simple channel with two symbols on the left of the channel $\{0, 1\}$ and two possible symbol states on the right $\{0, 1\}$, where p represents the probability of the correct symbol being received and q represents the probability of the incorrect symbol being received; as there are only two possible states the probability of p and q combined are equal to 1. Furthermore, it can be observed that the noise affects both symbols equally, therefore creating the symmetry such that $P(y = 1|x = 0)$ is equal to $P(x = 0|y = 1)$, represented by q and also that $P(x = 1|y = 1)$ is equal to $P(x = 0|y = 0)$, represented by p.

The toy example shown in figure 2.2.1 could be seen to represent a binary modulation scheme, such as Binary Phase Shift Keying (BPSK) or Binary Frequency Shift Keying (BFSK) where the transmitted symbol only varies one parameter of the medium

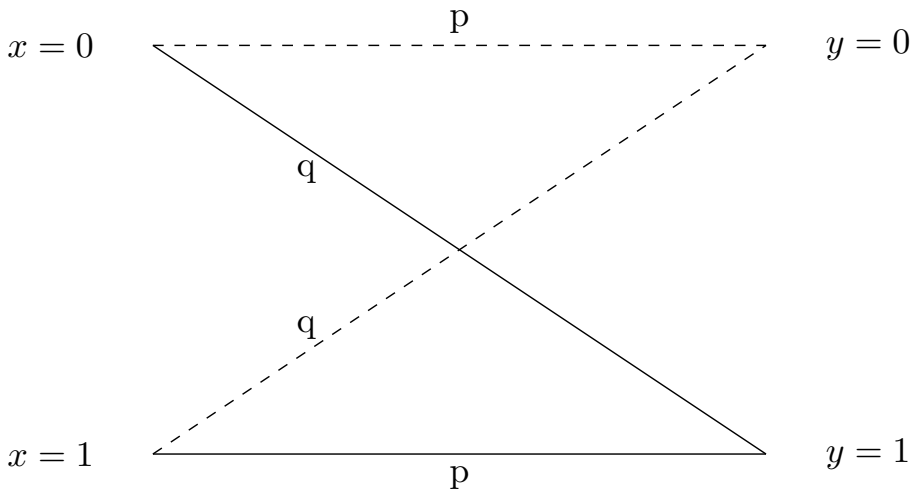


FIGURE 2.2.1: An example of a Discrete channel: The Binary Symmetric Channel

between two known states (ideally orthogonal in nature, to reduce the effects of channel impairments). In the case of BPSK this is achieved via the transmission of symbols that are orthogonal in phase of a signal, that is to say that the symbol representing $x = 0$ is 180° out of phase with that representing $x = 1$.

However as we wish to increase data rates, we would look to use M-ary modulation schemes such that $log_2(M)$ bits of information are contained within one transmitted symbol. That is to say, if 4 symbols are used, only 2 bits would be mapped to each symbol, equally if 4096 symbols were used then 12 bits of information could be contained within each symbol. It is this improvement in M-ary modulation schemes that will facilitate high data rate modes, such as the 4096-QAM mode proposed in 802.11be (Wi-Fi 7) [160].

However this increased data rate comes at a cost, specifically the channel capacity, as there is a trade off between Signal to Noise ratio and maximum noise free communications, this capacity was derived by Shannon in [119] as function of Signal to Noise ratio and bandwidth shown in Eq. (2.5). Where Bandwidth is defined in Hz, and SNR is defined as the ratio between the signal power and the noise power in a unitary bandwidth in dB.

$$C = B \log_2(1 + \frac{S}{N}) \tag{2.5}$$

As has already been shown the maximum rate of error free communications of any given modulation scheme is defined as $log_2(M)$ where M is the modulation depth, with the Capacity bound as defined in Eq. (2.5) it is therefore possible to simulate the

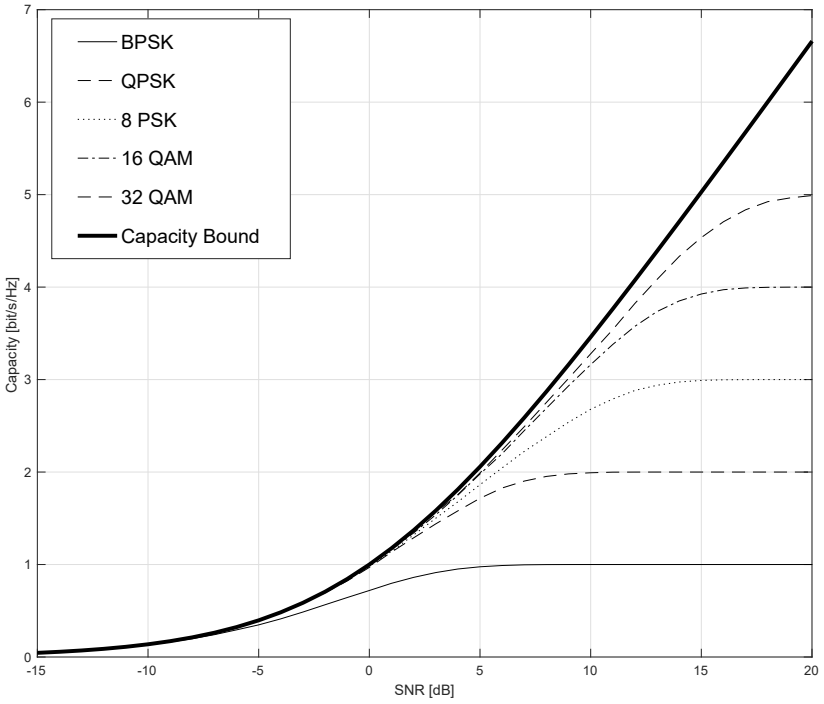


FIGURE 2.2.2: Channel Capacity and Capacity of Different Modulation Schemes

error free capacity in bits/s/Hz[3] of various different M-ary modulation schemes, as can be observed in figure 2.2.2.

Within figure 2.2.2 it is possible to observe the continuous-input continuous-output capacity of an AWGN channel represented by the thick black capacity bound compared to the Discrete Input Continuous Output Memoryless Channel (DCMC) capacity of various quadrature amplitude modulation and phase shift keying modulation schemes.

2.3 Security

Traditionally, security is considered a distinct component in the communications block diagram and processing chain. This separation typically arises from the use of a cryptographic processing unit or, in the case of many modern communications systems, application or IP layer security. It is not conventionally integrated within the Physical layer.

In Chapter 4, we will explore the concept of incorporating Physical Layer techniques with genuine cryptographic processing to establish a certain level of assurance for the three tenets of Information Security initially proposed in [161]:

[3]This is assuming the signal is in the exact same bandwidth as the noise, so the Bandwidth is unity.

- **Confidentiality;**
- **Integrity;**
- **Availability.**

These fundamental principles are also complemented by supplementary concepts, including:

- **Non-Repudiation;**
- **Authentication.**

A discussion of these tenets and concepts follows.

2.3.1 Confidentiality

Confidentiality, a cornerstone of security, involves safeguarding sensitive information from unauthorised access or disclosure [162; 163]. It ensures that data is accessible only to those with the appropriate permissions or clearances, protecting it from potential adversaries or unintended recipients. In the digital realm, this often involves employing encryption techniques and access controls to restrict data access to authorised individuals or systems. Confidentiality not only shields proprietary business information, intellectual property, and personal data from compromise but also fosters trust in systems, whether they are organisational networks, communication channels, or personal devices. As a fundamental tenet of security, confidentiality plays a crucial role in preserving privacy, maintaining the integrity of sensitive data, and upholding the overall resilience of information systems in the face of evolving threats.

2.3.2 Integrity

Integrity, a fundamental tenet of security [164; 163], revolves around maintaining the accuracy, consistency, and trustworthiness of data throughout its lifecycle. In the context of information systems, integrity ensures that data is not subject to unauthorised alteration, corruption, or tampering. This safeguard is crucial in upholding the reliability of information, whether it pertains to financial records, critical infrastructure controls, or user-generated content. Implementing mechanisms such as checksums [165], digital signatures [166], and access controls helps detect and prevent unauthorised modifications, thereby preserving the authenticity of the information. The assurance of data integrity not only fortifies the dependability of systems and the trust users place in them but also serves as a vital defence against

malicious activities that seek to compromise the accuracy and reliability of stored or transmitted information. In essence, integrity forms an indispensable foundation for the overall security and functionality of information ecosystems.

2.3.3 Availability

Availability, a crucial tenet of security [162; 163], focuses on ensuring that authorised users have timely and uninterrupted access to the resources and services they require. It emphasises the resilience of systems and networks, striving to prevent or minimise disruptions caused by various factors such as hardware failures, software glitches, natural disasters, or malicious attacks [167]. Robust redundancy measures, fault tolerance mechanisms, and strategic backup and recovery strategies [168] are implemented to mitigate the impact of potential disruptions and to maintain continuous service availability. Whether in the context of critical infrastructure, business operations, or digital services, ensuring availability is essential for sustaining productivity, preventing downtime, and preserving the functionality of systems. This tenet recognises that security is not solely about restricting access but also about ensuring that legitimate users can reliably access the resources they need when they need them.

2.3.4 Non-Repudiation

Non-repudiation, a pivotal principle in security [169], is centred on preventing individuals from denying the authenticity or origin of their own actions or communications. It establishes a level of accountability and trust by ensuring that parties involved in a transaction or communication cannot later disavow their participation. In digital communication and cryptographic contexts, non-repudiation is often achieved through mechanisms such as digital signatures [170] or cryptographic proofs [171]. These technologies provide irrefutable evidence of the sender's identity and the integrity of the transmitted information, making it nearly impossible for the sender to deny their involvement. Non-repudiation not only bolsters the reliability of electronic transactions but also holds legal significance in contractual agreements and digital interactions. This concept is integral in situations where establishing and maintaining trust and accountability are paramount, contributing to the overall robustness and credibility of security measures.

2.3.5 Authentication

Authentication, a fundamental concept in security [172], involves the verification of the identity of entities, such as users, systems, or devices, to ensure that they are who they

claim to be. The goal of authentication is to establish trust and control access to resources, systems, or information based on verified identities. Various authentication methods exist, ranging from traditional username and password combinations to more advanced techniques such as biometric identification, multifactor authentication, and cryptographic protocols. The authentication process typically involves presenting credentials, which are then validated against stored or pre-registered information. Strong authentication practices are essential for preventing unauthorised access, protecting sensitive data, and maintaining the overall integrity and security of systems. In digital environments, robust authentication mechanisms are a critical component of a comprehensive security strategy, forming a frontline defence against unauthorised access and potential security breaches.

2.3.6 Link between Security and Resilience

In section 2.1, a brief introduction into the aspects that affect the performance of communications in a noisy environment was given.

At first glance, this can seem drastically opposed to that of security, briefly introduced in Section 2.1.1, in that with resilient communications systems, we are trying to reduce any ambiguity within the search space for a receiver to decode and infer what information content was sent. On the other hand, with security, we are trying to increase this search space so that only intended receivers know the content of the message.

As mentioned earlier in Section 2.1, traditionally security approaches would happen further up the stack in the Open Systems Interconnection (OSI) model, either at Layer 6/7 (Presentation/Application) with an encrypted data format [4], or at Layer 3 (Network) via some form of IP Packet encapsulation. However, with wireless communications systems, this can only be done once a firm decision is made on what the inferred bit-wise message is. In practice, this approach suffices for wired communications or wireless communications whereby an IP protocol stack is used, as this firm or hard decision is made before a packet reaches any security processing.

However, if security approaches can be embedded into the symbol mapping and other low-level communications processes to change the mapping inferred in signal space, then it would be possible to enable flexible processing in data rate-limited environments with security throughout the entire communications system. If this mapping formed part of a shared key, a shared secret, then the receiver would be able to understand what was inferred by the transmitter whilst maintaining the **confidentiality** and **authentication** of the message; while the **integrity** of the

[4]Data Formats are simply a method of Source Coding, however traditionally not much emphasis is put on near-entropy coding in most data formats, with the exception of Imagery, Video and Audio formats

message was assured by appropriate channel and source coding, and the **availability** was ensured by having an approach to communications that was able to overcome the noisy channel. Unfortunately, **non-repudiation** would need to be part of a higher layer messaging protocol (or in-built memory or ledger), as this, in turn, requires other nodes to be able to provide confirmation that a message was indeed sent or not.

This approach to embedding security in the signal space will be explored further in Chapter 4.

2.4 Entropy and Mutual Information

2.4.1 Entropy

In the realm of information theory, entropy serves as a fundamental metric, embodying the inherent uncertainty within a system and offering insights into the nature of information sources. As a quantitative measure, entropy delineates the average amount of unpredictability associated with a set of potential outcomes, providing a nuanced understanding of the information content within a given context. Its application extends beyond mere probabilistic models, permeating diverse domains such as communication theory, cryptography, and data compression. Entropy, in the information theoretic sense, was originally proposed by Claude Shannon in [132] as a metric that could be used to understand how predictable various information sources are and how much information they truly provide.

The concept of a source having high entropy implies that if something is very predictable and occurs very often, then it has a low information content and, therefore, low entropy. Conversely, if an event is very rare, when it occurs, a lot of information is contained within said event.

2.4.2 Cross-Entropy of a Source

The cross-entropy of a source provides valuable insights into the inherent randomness of the source, offering a measure that helps us grasp both the unpredictability of the source and, concurrently, discern the theoretical minimum for the average bits per symbol that the source could achieve.

The cross-entropy of a source can be defined by Eq. (2.6). Shannon showed in [132] that the cross-entropy of the English language is 4.1, corresponding to the value measured if we take the cross-entropy of the source shown in figure 2.1.3.

$$H(p) = -\sum p(x) \log_2 p(x) \tag{2.6}$$

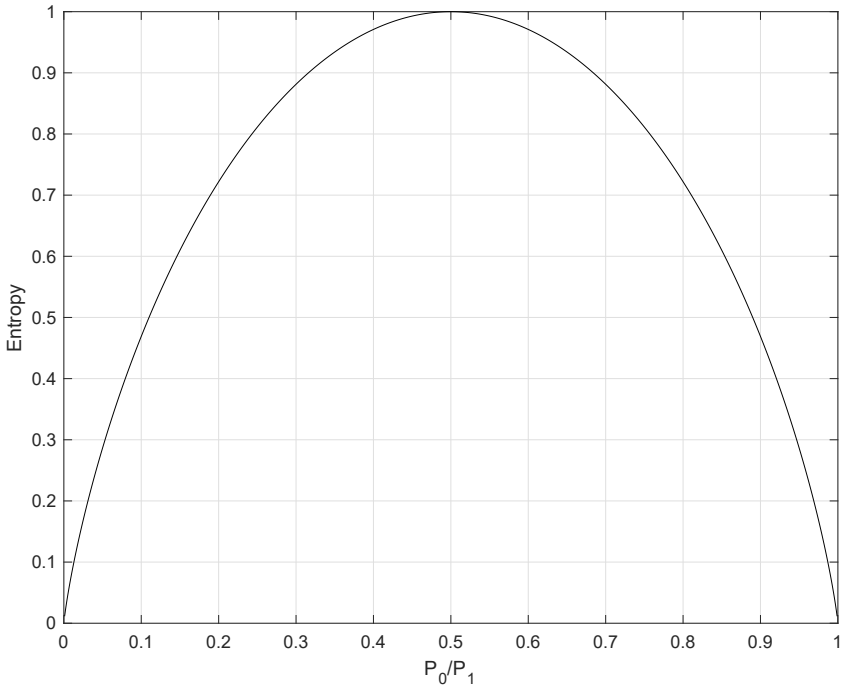


FIGURE 2.4.1: Relationship between Entropy and P_0/P_1

The entropy of a binary source, whether manifesting as the 1's and 0's in a digital communications system or the outcome of flipping a coin between heads and tails, is a concept crucially defined and measurable within the framework of information theory. This entropy characterises the degree of uncertainty or randomness associated with the source, serving as a quantitative indicator of the information content and unpredictability inherent in the binary outcomes. In the context of digital communication or probabilistic events like coin flips, understanding and quantifying this entropy becomes pivotal for optimising the transmission of information.

Taking Eq. (2.6) and applying it to the specific binary distribution, where we only have two possible probabilities leads to Eq. (2.7).

$$H = -P_0 \log_2 P_0 - P_1 \log_2 P_1 \tag{2.7}$$

This leads to a plot that can be seen in figure 2.4.1. In this plot, it can be seen that the Entropy of a binary source can only ever reach a maximum value of 1 bit, corresponding to $\log_2(2)$ as it is a binary choice. It can also be observed that this maximum is reached when there is a 50% chance of the output being a 0 or a 1.

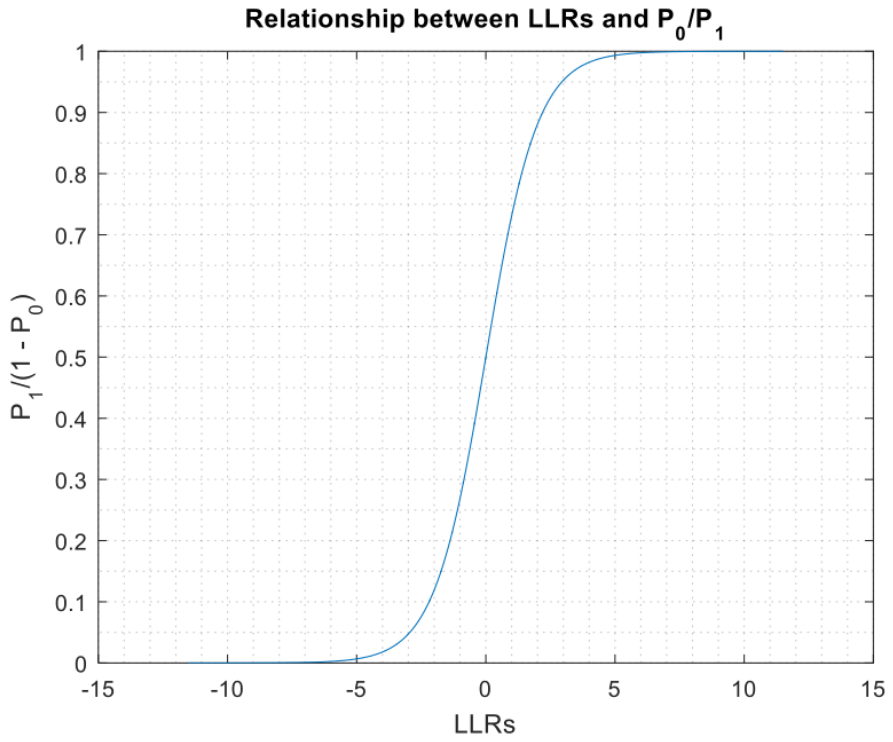


FIGURE 2.4.2: Relationship between LLRs and P_0/P_1

2.4.3 Log Likelihood Ratios

To evaluate the performance of communication schemes, it is essential to comprehend the evolution of information quality throughout the decoding process. This necessitates defining a measure of information for each discrete symbol.

The LLR serves this purpose, representing the ratio of the probability of the received symbol being 0 or 1. This is calculated using Eq. (2.8).

$$\text{LLR} = \frac{Pr(B_k = 1|\hat{B})}{Pr(B_k = 0|\hat{B})} \tag{2.8}$$

Where $Pr(B_k = 1|\hat{B})$ represents the probability of receiving the transmitted Bit $\hat{B}$ as a '1' valued bit B_k, and $Pr(B_k = 0|\hat{B})$ represents the probability it is received as a '0' valued bit.

As illustrated, when the probability of a symbol being 0 or 1 is 50%, an LLR of 0 is produced, representing the state of maximum entropy. This relationship is depicted in figure 2.4.2.

An important consideration is how the values for P_0 and P_1 are calculated, as this can impact the scaling of LLRs. Improperly scaled LLRs may lead to a receiver being overly optimistic or pessimistic in its LLR generation. To address this, it is crucial to

ensure the accuracy of LLRs. Fortunately, validation can be performed in a test environment where a priori symbols are known. This validation involves comparing two methods of LLR generation: one with absolute knowledge of the transmitted symbols (referred to as the histogram method) and one with no knowledge of the transmitted symbols (referred to as the averaging method). This technique is further discussed in Section 4.1.

2.4.4 Mutual Information

Mutual Information (MI) serves as a valuable metric to assess the performance of communication systems at various stages in the receiving chain. Specifically, it is employed to gauge the quality of LLR and determine the certainty of whether an inferred received symbol is correct.

Mutual information is always within the range (0,1), where 1 signifies 100% certainty that the symbol is correct, and 0 indicates a high level of ambiguity with a 50% certainty that the symbol is correct. It is noteworthy that if there is 0% certainty that the received symbol is not the intended symbol in a binary symbol mapping, then there is 100% certainty that it is the opposite symbol.

The MI is quantified by:

$$MI = 1 - H \tag{2.9}$$

Where H is the entropy of the LLRs. Combining Eq. (2.9) and Eq. (2.7) yields the comprehensive expression for Mutual Information in Eq. (2.10):

$$MI = 1 - (-P_0 \log_2 P_0 - P_1 \log_2 P_1) \tag{2.10}$$

Here, P_0 and P_1 represent the probabilities of the specific LLR being decoded as 0 or 1, respectively.

The specific relationship between P_0/P_1 and Mutual Information is illustrated in figure 2.4.3, where it can be observed that mutual information reaches a maximum when P_0 or P_1 is at 0 or 1, indicating absolute certainty that a 1 or 0 has been sent. Conversely, mutual information is lowest when P_0/P_1 is at 0.5, signifying absolute uncertainty about the original bit.

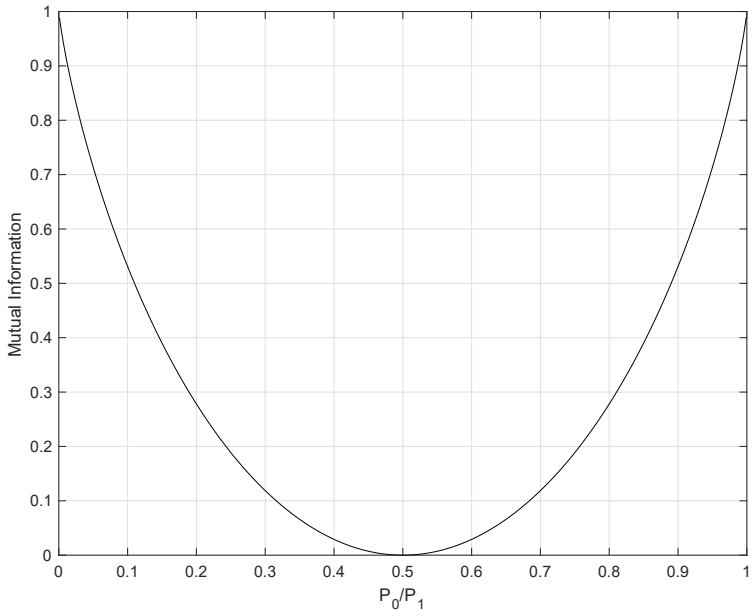


FIGURE 2.4.3: Relationship between Mutual Information and P_0/P_1

2.4.5 EXIT Charts

EXIT charts, introduced by ten Brink in [103], are a common method for analysing iterative decoders. They effectively represent the flow of information between constituent components of an iterative receiver.

Iterative decoding, a fundamental concept in modern error correction, involves multiple decoding iterations and the exchange of information between various decoder modules. The extrinsic information transfer refers to the information shared among these modules during the iterative decoding process. EXIT charts serve as graphical representations of this information transfer, mapping the relationship between input and output extrinsic information for a given decoder module. An example EXIT chart is shown in figure 2.4.4.

The chart employs two axes, as illustrated in figure 2.4.4, with one axis representing input extrinsic information and the other representing output extrinsic information. This graphical representation offers a comprehensive visualization of how the decoder transforms information during iterations, providing insights into convergence behaviour and decoding performance. Engineers and researchers leverage EXIT charts for in-depth analysis and design optimization of iterative decoding systems.

The information that is 'a-priori' (i.e. the input LLRs into a decoder) is referred a I_A and is shown on the y-axis, with the 'extrinsic' information, that which is the output of a decoder is referred to as I_E which is the x-axis. In the case of figure 2.4.4 the dark line represents the EXIT function of the inner decoder, the outer decoder can be

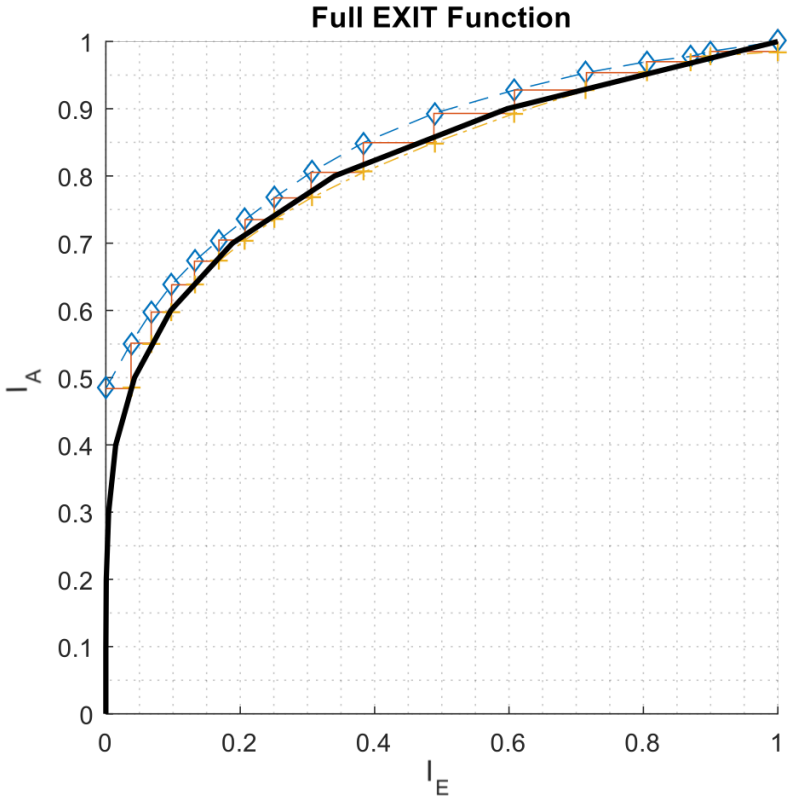


FIGURE 2.4.4: Example LDPC EXIT Function

represented on the same axis however is represented as the 'Inverted EXIT' whereby the I_A and I_E are inversed. In this case, the axis labels remain that of non-inverted EXIT and a text description will describe this labelling. These axis and definitions remain the same for all EXIT charts in the thesis.

Each curve on an EXIT chart depicts the mutual information between the input code of one component and the output of another. An illustrative example is provided by an LDPC decoder, as shown in figure 2.4.5.

In this scenario, it is feasible to construct an EXIT chart from both the Variable Node Decoder (VND) and the Check Node Decoder (CND) by assessing the mutual information at a_e and a_a. These variables signify the quality of the information being transmitted to and from the (VND). Mutual information gauges the correlation between a sequence of LLRs and a sequence of bits. A mutual information value of 1 implies that all LLRs possess high quality, displaying correct signs and significant magnitudes. Conversely, a mutual information value of 0 indicates low-quality LLRs, characterised by random signs and low magnitudes.

By examining the quality of mutual information at these points or generating LLRs at a_a to represent a specific input LLR quality and measuring the output LLRs at a_e, it becomes possible to derive the EXIT function of the composite decoder. This process

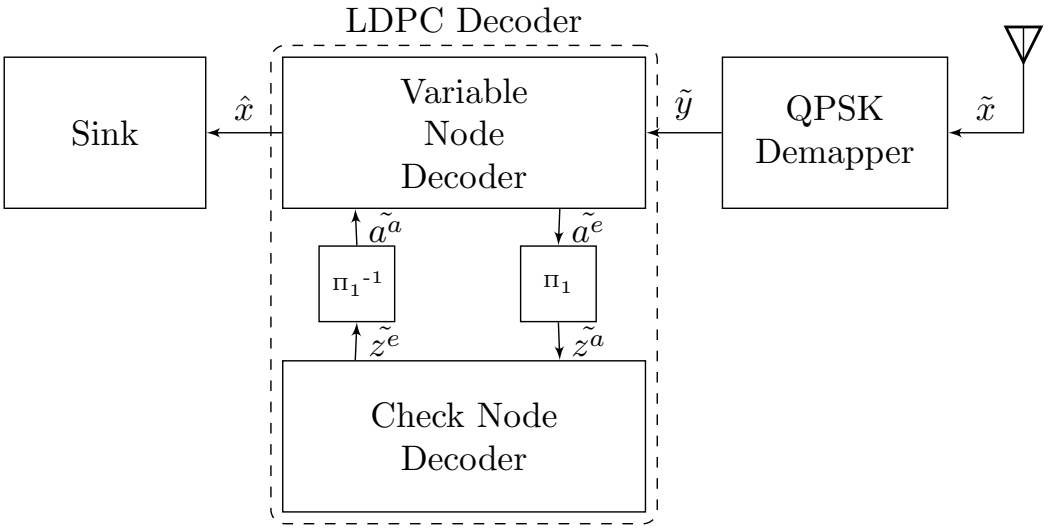


FIGURE 2.4.5: LDPC Decoder Architecture

can be repeated for the (CND). Notably, the axes are switched for one of the component codes, as the input of one component code becomes the input of the other. This axis switch allows both EXIT curves to be simultaneously presented on the same chart.

EXIT 'Trajectories' can then be plotted between the curves to map the progress of decoding in a single block. If the trajectory is blocked by the overlapping of curves, for example in a noisy channel with a low quality of channel information, then successful decoding is impossible.

Furthermore, it has been shown in [173] that the area between the EXIT curves (assuming that the inner code has a rate of 1) is shown to be the distance to Channel capacity. Further descriptions of EXIT functions can be found in [174].

2.5 Standards

To achieve operational effectiveness in various environments, whether civilian or defence-oriented, seamless communication among all actors is imperative. This requirement has been evident throughout history, from naval ships using semaphore flags during the Battle of Trafalgar in 1805 [175] to the people of ancient Mesopotamia employing Sumerian for market trade [176]. In contemporary scenarios, such as autonomous systems ensuring safe urban transportation [177], effective communication remains paramount. The foundation of effective communication lies in achieving a shared understanding, encompassing the manipulation of transmission mediums (such as voice, flags, writing, radio, or acoustic signals), the mapping of symbols to the

observer's comprehension (whether human or machine), and adherence to grammatical structures governing the arrangement of these symbols. Additionally, considerations extend to the sequencing and pace at which actors present information.

This pursuit of shared understanding is akin to establishing a standard, encapsulated in documents like the Oxford English Dictionary [178] or, in the realm of digital communications, within standards like those defined by 3GPP for 5G New Radio [148]. The use of standards is pivotal in enabling all engaged actors to interpret and exchange information effectively, contributing to the coherence and efficiency of various activities.

The requirement to develop standards is key to enabling communication 'capability' from the proposed systems within this thesis, and the theme of standards will be revisited throughout the thesis, particularly in chapters 4 and 5, where the techniques proposed directly relate to NATO standardisation efforts.

2.6 Chapter Conclusion

Within this chapter, the reader has been provided a high-level overview of some key technical subject matter that is relevant to the remainder of the thesis, specifically the topics of source distributions, source coding, channel coding, modulation, security and standards have been introduced.

In the next chapter of the thesis, we delve into the depths of source and channel coding. Alongside EXIT chart analysis, where the reader will be presented with the novel Reordered Exponential Golomb Joint Source Channel Code.

Chapter 3 : Reordered Exponential Golomb Joint Source Channel Coding

Joint Source Channel Code (JSCC) is a powerful technique that allows for the efficient transmission of information by simultaneously considering the characteristics of both the source and the channel.

The recently proposed Exponential Golomb Error Correction (ExpGEC) [140]and Rice Error Correction (REC) [142] codes provide generalised JSCC schemes for the near capacity coding of symbols drawn from large or infinite alphabets. Yet, these require impractical decoding structures, with large buffers and inflexible system design, this was mitigated by the introduction of the Reordered Elias Gamma Error Correction Code (REGEC) [106] which itself had limited flexibility in regard to source distribution.

Within this chapter, the novel RExpGEC coding scheme is proposed, which is a JSCC technique designed for flexible and practical near-capacity performance. The proposed RExpGEC encoder and decoder are presented, and its performance is analysed using Extrinsic Information Transfer charts. The flexibility of the RExpGEC is shown via the novel trellis encoder and decoder design. Finally, the symbol error rate performance of RExpGEC code is compared when integrated into the novel RExpGEC-URC-QPSK scheme against other comparable JSCC and SSCC benchmarkers.

Specifically the RExpGEC-URC-QPSK scheme is compared against the REGEC-URC-QPSK scheme, and a serial concatenation of the Exponential Golomb and Convolution Code, which becomes the novel ExpG-CC-URC-QPSK scheme. Our simulation results demonstrate the performance gains and flexibility of the proposed RExpGEC-URC-QPSK scheme against the benchmarkers in providing reliable and efficient communications.

The RExpGEC-URC-QPSK scheme outperforms the SSCC in an uncorrelated Rayleigh fading channel by 2 to 3.6 dB (dependent on source distribution).

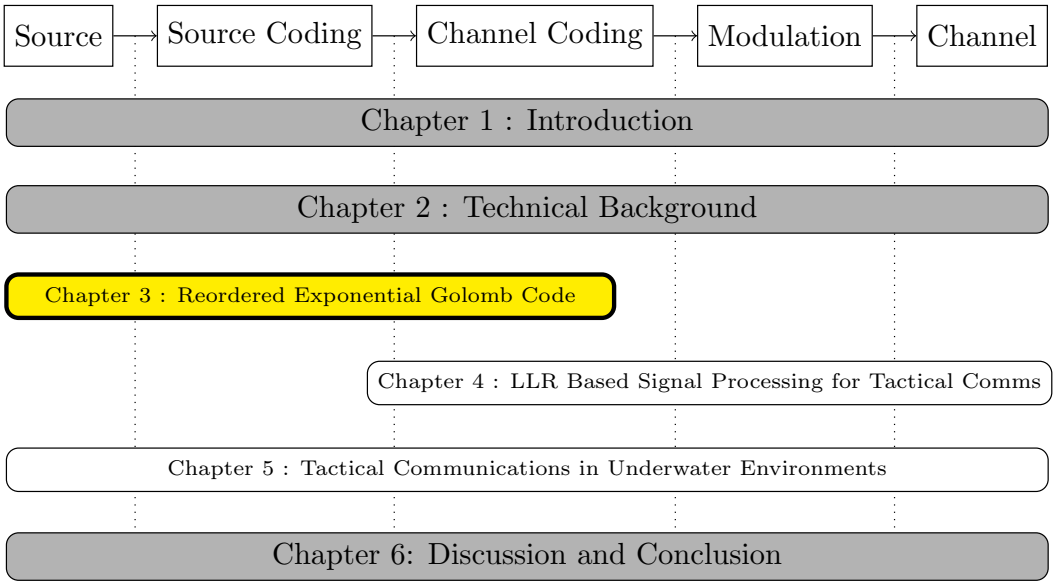


FIGURE 3.1.1: Structure of the Thesis

Furthermore, the RExpGEC-URC-QPSK scheme consistently operates within 2.5 dB of channel capacity when measuring E_b/N_0, whilst providing flexibility in SNR performance when compared to the REGEC-URC-QPSK scheme. These performance gains come at the cost of complexity, whereby the RExpGEC-URC-QPSK scheme is 3.6 times more complex than ExpG-CC-URC-QPSK scheme under certain conditions.

Chapter 3 can be seen highlighted within the structure of the overall thesis in figure 3.1.1, whereby Chapter 3 focuses predominantly on source and channel coding techniques before leading into Chapter 4 which focuses on the LLR Based Signal Processing and Chapter 5 where the focus is on modulation schemes for underwater communications.

A large part of Chapter 3 is published in [4] and the work presented in this thesis represents the sole work of the author of this thesis.

This chapter emphasises the unique features of the RExpGEC and its ability to offer near-capacity flexible source and channel coding. A visual structure of the chapter can be seen in figure 3.1.2 demonstrating the flow of the discussion within this chapter. The rest of the chapter is organised as follows. We provide an introduction to the novel RExpGEC code in Section 3.2, where we highlight the novel contributions both around the development of a universal JSCC that can be flexibility adapted to different source distribution and has a finite low complexity decoder even when the source alphabet is large or infinite. In Section 3.3 we exemplify a novel concatenation of the RExpGEC with a URC inner code and QPSK modulation, known as the RExpGEC-URC-QPSK scheme, to achieve near-capacity performance. Furthermore,

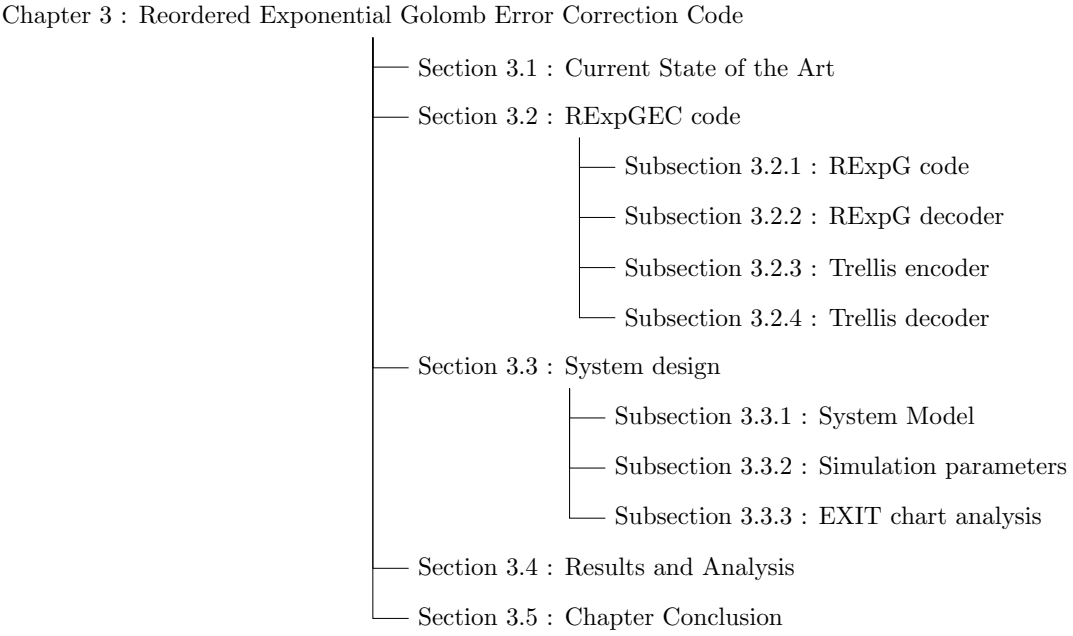


FIGURE 3.1.2: Structure of Chapter 3

Section 3.3 also provides novel contributions presented based on the EXIT chart analysis of the RExpGEC outer and URC inner code to enable the near-capacity design of the inner code and predict symbol error rate performance. In Section 3.4 we then compare the symbol error rate results against a series of benchmarkers in order to understand the relative and absolute performance of the RExpGEC scheme. Finally, we conclude the chapter in Section 3.5.

3.1 Current state of the art

The modern world relies heavily on information content and reliable access to information transfer of large data sources. In order to transmit this information over noisy wireless communications links via reliable means, information sources are typically encoded via a process known as source coding in order to compress them. Then these sources are separately encoded to enable redundancy and robustness by channel coding. This process, originally postulated by Shannon in [119] utilises SSCC which can theoretically achieve near capacity operations. In SSCC a separate near-entropy source code, such as the Lempel-Ziv code [122], Elias Gamma [179], Huffman [144], Golomb [107], Shannon-Fano [131] codes, or many other possible source codes [180; 181; 182; 183], can be utilised with a separate channel code, such as a turbo code [124; 140], Polar Code [184], LDPC code [125], or any number of channel codes [126; 127; 128; 129; 130; 131] to theoretically achieve near-capacity performance. However in order to achieve near-capacity performance these near-entropy source codes become infinitely complex, extraordinarily large in block size [185] or require large

processing times [186]. For example, the Lempel-Ziv code [122] requires accurate knowledge of the entire source and associated symbol probabilities before a single bit can be transmitted to the receiver. Equally with SSCC, a single bit in error, or a dropped packet can cause the entirety of the information to be lost. Therefore, not only must a robust channel code be utilised, but error checking and higher layer signalling must be employed to ensure the entire message is received.

For the transmission of information, whereby the source distribution is not known apriori, there is strong motivation for the use of universal codes for source coding [187], which provide finite codeword lengths irrespective of source distribution, provided the source is monotonically distributed. This family of codes are known as universal codes, and include Elias Gamma [179], Fibonacci Code [188] and the Exponential Golomb (ExpG) code [189]. These universal codes operate without any knowledge of the source symbol probabilities. However, non-negligible redundancy remains in the encoded bitstreams, which in turn leads to capacity loss when treated as a separate source and channel problem. This capacity loss motivates a JSCC [190] whereby the residual redundancy from the source coding can be utilised to enhance the attainable error correction capability.

State of the art JSCC techniques, such as the Reordered Elias Gamma Error Correction Code (REGEC) [106] have been demonstrated to show near capacity performance for both large and infinite cardinality sources. However, they are only designed for a limited range of probability distributions, approximating specific zeta distributed sources which are psuedo-monotonic in nature (where successive symbols have successively lower symbol probabilities). This limitation meant that outside of these source distributions the REGEC code offers poor coding efficiency.

The Exponential Golomb Error Correction Code (ExpGEC) code introduced in [142] is parametrizable, whereas the Elias Gamma code used in the REGEC code of [106] is a special case of this with fixed parameters. Therefore, the ExpGEC is more generalised and has greater flexibility for different source distributions. However, the proposed scheme requires a series of buffers to realise, due to the structure of the ExpG code and its variable length nature. Furthermore, the proposed scheme had high complexity and the ExpGEC could not be represented using a single finite complexity decoder, as could be done with the REGEC in [199]. A summary of relevant and major contributions in the field of channel coding, source coding, and JSCC is presented in Table 3.1.1.

In this chapter, we propose the RExpGEC code, which attempts to tackle these problems, and presents a novel highly flexible JSCC that can be used for diverse probability distributions with a large of infinite source cardinality. The proposed RExpGEC is able to be realised in a finite complexity decoder attaining near-capacity performance for a variety of source symbol distributions. We further illustrate the performance and flexibility of the novel RExpGEC by providing simulation results of

TABLE 3.1.1: Relevant and major contributions in source and channel coding

Year	Author	Contribution
1948	Shannon, C.[119]	The foundations of information theory
1952	Huffman, D.A [144]	Huffman source code
1960	Reed, I.S.; Solomon, G. [130]	Reed-Solomon channel code
1962	Gallager, R. [125]	Original LDPC channel code
1967	Viterbi, A.J. [129]	The Viterbi decoding algorithm
1975	Elias, P. [179]	Elias Gamma source code
1977	Massey, J.L [190]	Non-iterative JSCC
1978	Ziv, J.; Lempel, A. [122]	Lempel-Ziv variable rate source code
1979	Rissanen, J [191]	Arithmetic source coding
1980	Stout, Q.F. [192]	The Stout source code
1988	Bernard, M.A [193]	The VLEC JSCC
1993	Berrou, C [124]	The Turbo channel code
1996	Fraenkel, A.S [188]	The Fibonacci channel code
2000	Bauer, R.; Hagenauer, J. [194]	Introduction of iterative decoding for VLECs
2000, 2001	Görtz, N [195; 196]	The introduction of iterative JSCC decoding
2009	Arikan, E. [184]	Polar channel code
2013	Maunder, R.G. [197]	The Unary Error Correction (UEC) JSCC
2013	Wang, T. [198]	The Elias Gamma Error Correction (EGEC) JSCC
2016	Wang, T. [106]	The REGEC JSCC
2016	Brejza, M. [142]	The Exponential Golomb Error Correction (ExpGEC) JSCC
2023	Hamilton, A. [4]	RExpGEC JSCC

the proposed scheme in an uncorrelated Rayleigh fading channel in comparison to a SSCC benchmarker.

Given the above background the novel contributions of this chapter can be summarised as follows:

1. We propose the novel RExpGEC coding scheme, which is a flexible near-capacity JSCC suitable for any pseudo-monotonic source distributions including diverse zeta-distributed sources;

2. We propose a novel trellis decoder designed for the proposed RExpGEC code which has a low and finite complexity even when symbols are drawn from a large or infinite alphabet;

3. We propose a novel iterative decoding scheme which exemplifies the concatenation of the RExpGEC with a URC inner code and QPSK Modulation (RExpGEC-URC-QPSK);

4. We present novel performance analysis of RExpGEC, measured by EXIT chart analysis initially developed in [103], and by symbol error rate performance when concatenated with a URC inner code and QPSK modulation;

5. We compare the Symbol Error Rate of the RExpGEC-URC-QPSK scheme performance to that of comparable JSCC and SSCC techniques.

Our findings illustrate the exceptional performance and flexibility of RExpGEC in delivering reliable and efficient communication over a wireless channel. Specifically, the RExpGEC outperforms the SSCC in an uncorrelated Rayleigh fading channel by 2 to 3.6 dB (dependent on source distribution), whilst providing a finite and low complexity that is flexible dependent on system design. Furthermore, we show that by increasing the parameterisation of the REGEC with the RExpGEC, the utility for different pseudo-monotonical source distribution improves, due to the ability to closer match the source distribution to the average codeword length and target the source coding performance of the RExpGEC.

3.2 Proposed RExpGEC Code

In this section, we introduce the novel RExpGEC code design and its constituent components, which are the novel RExpG encoder and the Trellis encoder which enables transition from RExpG to RExpGEC, as well as the corresponding novel trellis decoder which enables a finite, low complexity and flexible decoder design for the RExpGEC.

The considered block diagram of the RExpGEC is shown in figure 3.2.1, where $\mathbf{x}$ represents the sequence of information symbols, $\mathbf{r}$ the sequence of RExpG encoded bits, and $\mathbf{z}$ the sequence of RExpGEC encoded bits. For the purpose of figure 3.2.1 the inner code functionality also constitutes modulation mapping and demapping for transmission over a wireless channel, as these can be seen as part of the generic inner code functionality for the RExpGEC.

Section 3.2.1 introduces the RExpG code, its design, and some of it's attractive qualities which enable the novel tree and trellis designs. Section 3.2.2 introduces our novel RExpG decoder, which operates on a novel tree representation of the RExpG code. This tree has a finite complexity which enables the design of a finite yet flexible trellis, which is used as the basis for RExpGEC decoder described in Section 3.2.4. Section 3.2.3 introduces the novel trellis structure design for the RExpGEC and how it is used to encode RExpGEC codewords. Section 3.2.4 introduces the novel trellis

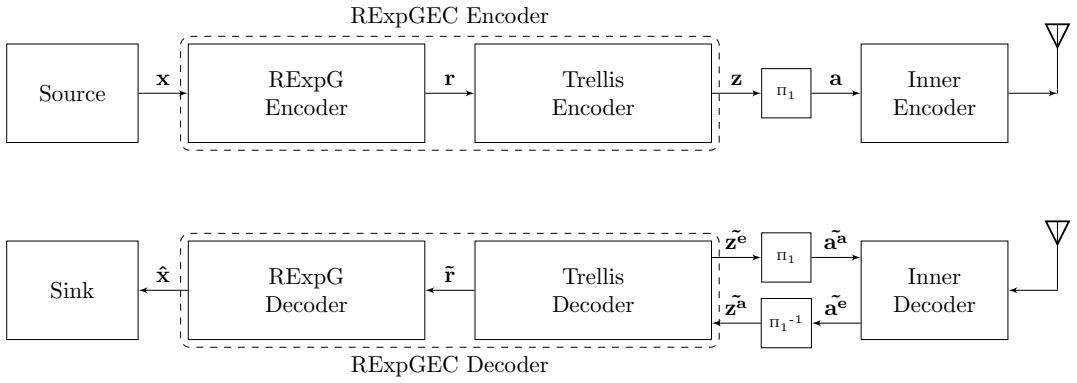


FIGURE 3.2.1: Generic Block Diagram of RExpGEC.

decoder for the RExpGEC and how it is used to decode RExpGEC codewords for near-capacity performance.

3.2.1 RExpG Code

The proposed novel Reordered Exponential Golomb (RExpG) code is a universal code which can work with large or infinite source sets, where each symbol in the source sequence $\mathbf{d}$ has a value (d_i) in the range 1 to L (where L is the cardinality of the source), where higher symbol values correspond to reducing probabilities. Each symbol is mapped to a RExpG codeword, where longer codewords are used for higher symbol indices. These symbols can be seen in Table 3.2.1 The code is parameterised by the k parameter, where $k \in (0, 1, 2, 3, \dots)$. This enables the code to have high-efficiency source coding for a variety of different distributed sources [200], as discussed in [142] where the authors discuss the information efficiency of the similar Exponential Golomb code for varying zeta-distributed sources. This ability to closely match a zeta distributed source enables the RExpG to be suited to a variety of different uses, such as video [106; 201], text [202] or imagery [203] which provides the RExpGEC with a wide flexibility for use with different source distributions.

The initial bit of the RExpG codeword is always a unary bit, following which the bits are subsequently interlaced between unary and FLC bits until the final unary bit is reached, this initial section of the codeword can be referred to as the 'combination' section of the codeword. The final k bits corresponding to the k parameter of the RExpG code itself will always be bits derived from the fixed length sub-symbol, where this section of the RExpG codeword can be referred to as the 'terminal' section of the codeword. This interlacing and construction can be observed in figure 3.2.2

As shown in Table 3.2.1 the bits in each RExpG codeword may be considered to derive from two groups, a unary part and a fixed length part, which are interlaced to create the RExpG codeword, in a manner shown in figure 3.2.2. For the purpose of

Reducing Probability

d_i	RExpG(d_i) k=0 Combi	T	RExpG(d_i) k=1 Combi	T	RExpG(d_i) k=2 Combi	Term	RExpG(d_i) k=3 Combi	Term
1	1		1	0	1	00	1	000
2	001		1	1	1	01	1	001
3	011		001	0	1	10	1	010
4	00001		001	1	1	11	1	011
5	00011		011	0	001	00	1	100
6	01001		011	1	001	01	1	101
7	01011		00001	0	001	10	1	110
8	0000001		00001	1	001	11	1	111
9	0000011		00011	0	011	00	001	000
10	0001001		00011	1	011	01	001	001
11	0001011		01001	0	011	10	001	010
12	0100001		01001	1	011	11	001	011
13	0100011		01011	0	00001	00	001	100
14	0101001		01011	1	00001	01	001	101
15	0101011		0000001	0	00001	10	001	110

Increasing Codeword length

TABLE 3.2.1: The decomposition of symbols d_i of the Reordered Exponential Golomb Codewords for $k \in 0, 1, 2, 3$ demonstrating the concatenation of the Mixed and Terminal codes. 'Combi' refers to the combination of interlaced FLC and Unary bits, 'T' and 'Term' both refer to the Terminal bits of the RExpG codeword.

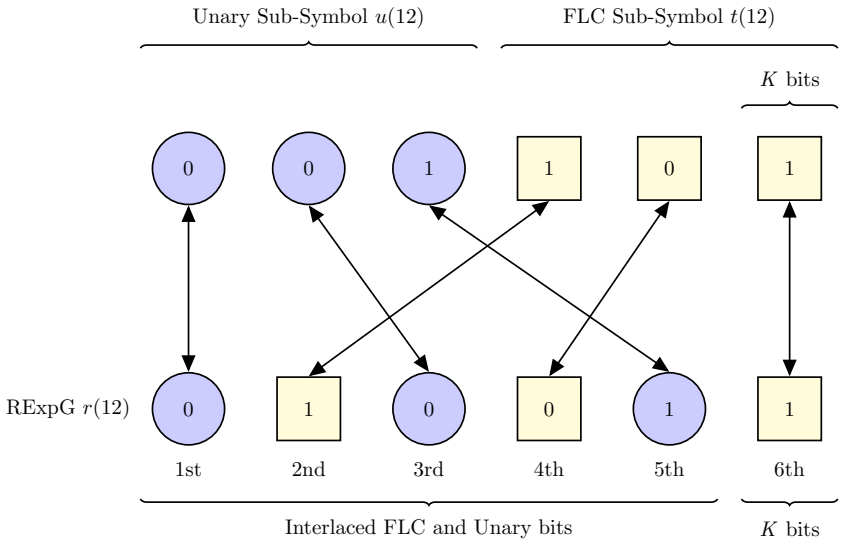


FIGURE 3.2.2: Construction of RExpG symbol $d_i = 12$ when $k = 1$.

d_i	ExpG(d_i) k=0 Unary	FLC	ExpG(d_i) k=1 Unary	FLC	ExpG(d_i) k=2 Unary	FLC	ExpG(d_i) k=3 Unary	FLC
1	1		1	0	1	00	1	000
2	01	0	1	1	1	01	1	001
3	01	1	01	00	1	10	1	010
4	001	00	01	01	1	11	1	011
5	001	01	01	10	01	000	1	100
6	001	10	01	11	01	001	1	101
7	001	11	001	000	01	010	1	110
8	0001	000	001	001	01	011	1	111
9	0001	001	001	010	01	100	01	0000
10	0001	010	001	011	01	101	01	0001
11	0001	011	001	100	01	110	01	0010
12	0001	100	001	101	01	111	01	0011
13	0001	101	001	110	001	0000	01	0100
14	0001	110	001	111	001	0001	01	0101
15	0001	111	0001	0000	001	0010	01	0110

Reducing Probability ↓

↓ Increasing Codeword length

TABLE 3.2.2: The decomposition of symbols d_i of the ExpG Codewords for k=0, k=1, k=2, and k=3 showing the concatenation of the Fixed Length Code and Unary codes.

illustration in figure 3.2.2 the bits which derive from the unary group can be referred to as the unary sub-symbol, and those from a fixed length the Fixed Length Code (FLC) sub-symbol. The bits which derive from the an underpinning Fixed Length Code (FLC), are shown in yellow in Tables 3.2.1 and 3.2.2 and figure 3.2.2 and referred to as u, whereas the bits which derive from a unary code are shown in blue in Tables 3.2.1 and 3.2.2 and figure 3.2.2 and are referred to as t.

The Unary Code, as used in the unary sub-symbol, is defined by a series of all zero-valued bits immediately followed by a single logical one-valued bit, which is subsequently referred to as the *terminal unary bit* which indicates the end of the Unary Code sub-symbol, the total length of the Unary code sub-symbol u is defined as $x(d_i)$.

$$x(d_i) = \lfloor log_2(d_i + 2^k - 1) \rfloor + 1 - k. \tag{3.1}$$

The Fixed Length Code sub-symbol is a representation of the bits which exist within a RExpG symbol which derive from the fixed length part and can be directly be calculated as the sub-symbol $t(d_i)$. The value of the fixed length sub-symbol is.

$$t(d_i) = d_i - 2^{\lfloor log_2(d_i + 2^k - 1) \rfloor} + 2^k - 1, \tag{3.2}$$

which is represented in binary form with a length exactly corresponding to $s(d_i)$.

$$s(d_i) = \lfloor log_2(d_i + 2^k - 1) \rfloor. \tag{3.3}$$

The RExpG codeword has a length as follows in Eq. (3.4), of which $x(d_i)$ of those are Unary bits, with the remainder $s(d_i)$ being FLC bits. This is the sum of the length of the Unary $x(d_i)$ and FLC $s(d_i)$ sub-symbols.

$$l(d_i) = x(d_i) + s(d_i) = 2 \times \lfloor log_2(d_i + 2^k - 1) \rfloor + 1 - k. \tag{3.4}$$

Based on Eq. (3.4), for the RExpG the *terminal unary bit* is set at a fixed k bit locations from the end of the codeword and preceding this every alternative bit is a Unary codeword. Therefore, there is always a known number of bits to the end of the codeword, which is k bits, following a logical one-value unary bit. This enables a finite complexity decoder to be utilised as will be detailed in Section 3.2.4.

To provide a specific example of a RExpG symbol, we visually describe the process for developing the RExpG symbol for $d_i = 12$ when $k = 1$ in figure 3.2.2, and how a transmitter can convert from symbol d_i to a RExpG codeword $r(d_i)$. This symbol $d = 12$,k= 1 will be utilised as an example throughout Section 3.2.

As can be observed in figure 3.2.2, initially the sub-symbol $u(12)$ is generated with a length of 3, as defined by Eq. (3.1), which generates the sub-symbol $0, 0, 1$ (as indicated by the blue bits), and the corresponding sub-symbol $t(12)$ with the integer value 5 as defined by Eq. (3.2) , which in binary form with a length defined by Eq. (3.3) is $1, 0, 1$ (as indicated by the yellow bits). Following this via the RExpG generation process these sub-symbols produce the RExpG codeword $0, 1, 0, 0, 1, 0$. Therefore the bits in location 2,4 and 6 originate from the Unary sub-symbol, whereas bits in location 1,3 and 5 originate from the FLC sub-symbol.

Table 3.2.1 shows the first 15 codewords for the RExpG code for $k \in 0, 1, 2, 3$. The colours represent the same colours as those used in figure 3.2.2, which will be the same colours used throughout the remainder of this chapter to represent bits which are derived from FLC and unary components.

Let us now compare our novel RExpG code with the ExpG code of [142], for which the first 15 codewords are shown in Table 3.2.2 and elaborate on the similarities and differences between the two codes. Whilst the structure of the RExpG code is generated from interlaced unary and FLC sub-symbols as described above, the structure of ExpG is composed simply of two concatenated sub-symbols $\mathbf{u(d_i)}$ and $\mathbf{t(d_i)}$, which represent a sub-symbol of Unary Code bits and a sub-symbols of Fixed Length Code bits respectively. As observed in Table 3.2.2 the location of the *terminal Unary bit* of each ExpG symbol $\mathbf{d(d_i)}$ in a sequence of symbols $\mathbf{D}$ is at an unknown location, as the *terminal unary bit* is located at a variable location from the end of each codeword, and preceded by an unknown number of logical zero-valued bits. This property motivates the design of the RExpG code, where in contrast, the *terminal unary bit* is at a known distance from the end of the codeword. As we will show in the

next sections, this known property of the RExpG can be exploited for designing a finite complexity decoder, rather than the infinite complexity decoder that is required for the ExpG.

The total rate R_o of the RExpGEC when compared with the original information source is a function of both the coding rate of the scheme, the modulation order, as well as the information efficiency (η). The information efficiency of different P_1 and k distributions of the RExpG can be seen in figure 3.2.3 where different P_1 and k distributions are shown. These difference η parameters, combined with the coding rate and modulation order, produce a CCMC capacity for the energy required per bit of information (based on the entropy of the information source) which differs according to the source distribution. For a monotonic source with P_1 of 0.6 and the k parameter of 0, this offers the highest information efficiency or η, which matches with the P_1 value chosen for the EXIT analysis presented in figures 3.3.2 to 3.3.4 in Section 3.3.3 and simulations presented in figure 3.4.2 in Section 3.4. However, for a different P_1 value, such as 0.3, other values of k offer better performance, and this can be observed in the results shown in figures 3.4.3 and 3.4.4 of Section 3.4.

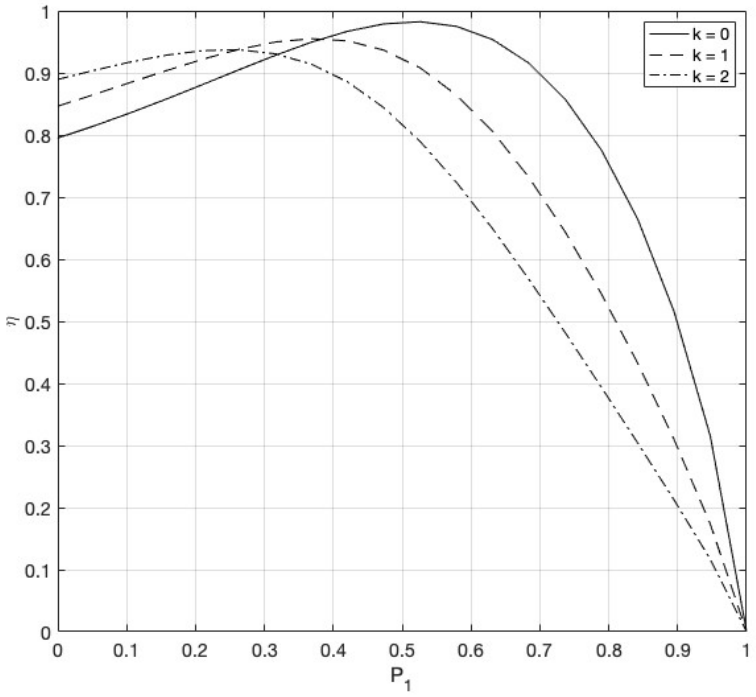


FIGURE 3.2.3: Information Efficiency (η) of RExpG with different Zeta distributions of infinite cardinality.

3.2.2 RExpG Decoder

In this section we introduce a method to decode a sequence of RExpG codewords via the RExpG tree decoder, which is illustrated in figure 3.2.4.

As discussed in Section 3.2.1, a key motivation for the RExpG (and associated RExpGEC) is to enable the serial decoding of a sequence of symbols **D** and to enable a finite yet flexible decoder design. In order to enable the RExpGEC to have a finite complexity decoder, one must have a finite sized binary tree, which can be achieved with the RExpG code and is described below.

In figure 3.2.4 the tree is represented visually, where each line represents a transition of the RExpG codeword whereby a dashed line represents a 0 bit valued transition and a solid line represents a 1 bit valued transition, and each coloured node represents either a FLC derived state (yellow square) or a unary derived state (blue circle), which are uniquely numbered. The white circles represent the leaf nodes, which indicate that a symbol has been reached. In the case of the tree in figure 3.2.4 which represents a depth of 1, there are 8 unique leaf nodes (also referred to as terminal nodes), with the final 2 leaf nodes representing all symbols above 7 depending on the *holding pattern*. A RExpG tree with a larger depth will have more unique leaf nodes and utilise the *holding pattern* less, as more symbols are likely to have unique paths through the tree.

Because of the design of the RExpG code, a tree can be designed in such a way with a *holding pattern*, which constitute a single FLC and Unary *holding state* with a circular transition as well as an exit and entry transition, as exemplified in figure 3.2.4 between states '7' and '9'. This is considered until the conditions of the Unary sub-symbol becoming a logical 1-valued bit can escape to a known FLC sub-tree, which is constant, as there are always a constant k FLC bits, following the *terminal unary bit*. This can be observed in figure 3.2.4, which shows the ability to enable a holding pattern at the *terminal unary bit*, which in turn enables a finite complexity tree to be achieved for the RExpG code.

Furthermore, where the value of k used in the tree in figure 3.2.4 is 1, the k parameter dictates the number of states in each FLC branch, which comes from unary states, when a logical one-valued bit is identified, indicating a *terminal unary bit*. This is exemplified in figure 3.2.4, where for states $'2', '6', '8'$ and $'10'$ these are the initial stages of an FLC branch. In this case, with the k parameter having a value of 1, there are 2 terminal nodes. Correspondingly, if k was 0 these nodes themselves would be only one terminal node, and if k was 2 there would be 2 FLC 'stages' and 4 terminal nodes.

This holding pattern is defined as the the recursive states between state number '7' and state number '9' in figure 3.2.4. The number of Unary branches which are before this holding pattern and therefore total number of states of the RExpG tree decoder

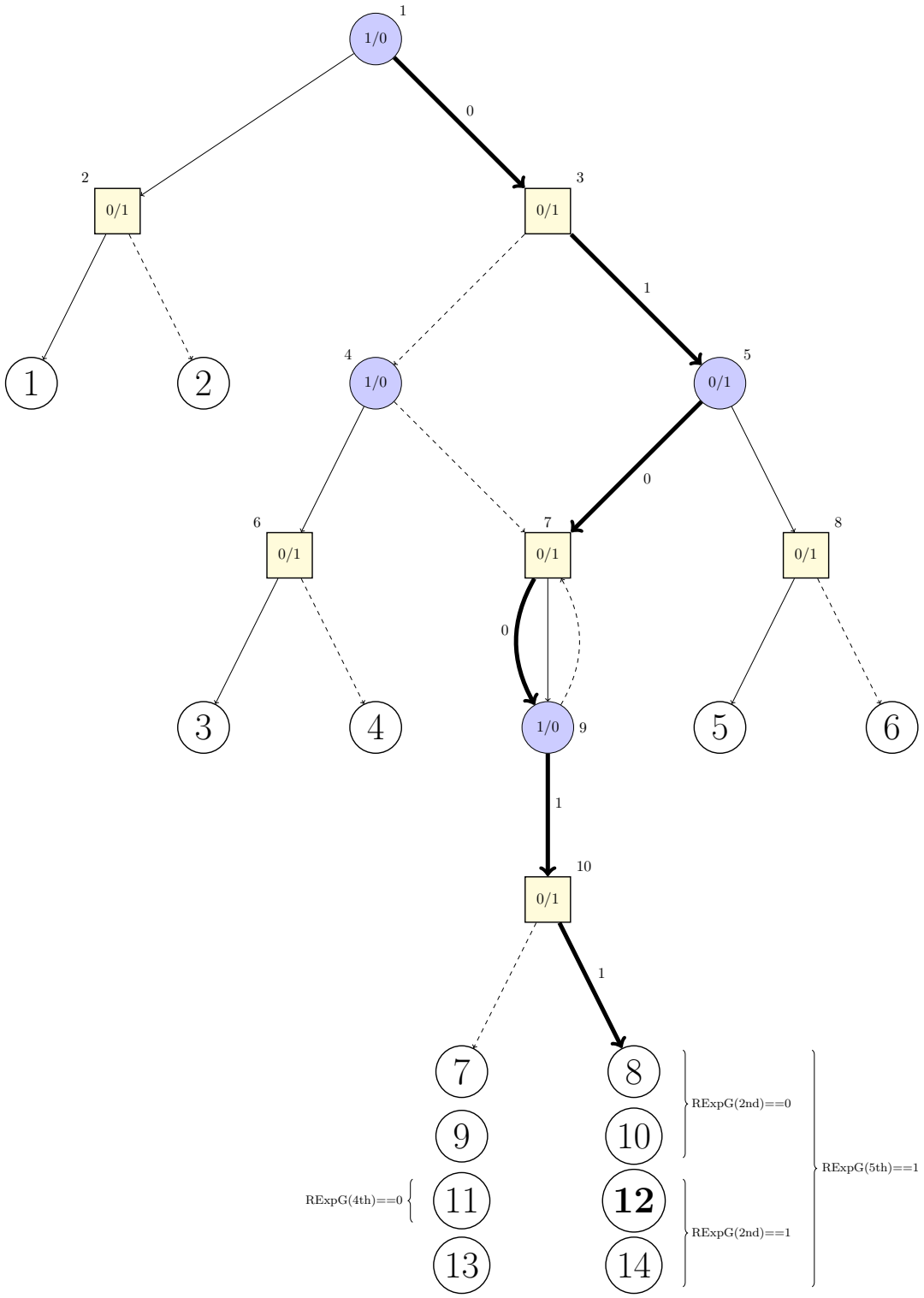


FIGURE 3.2.4: RExpG Tree Decoder with a tree depth of 1, and an example of decoding the RExpG symbol with values RExpG k=1, d_i=12.

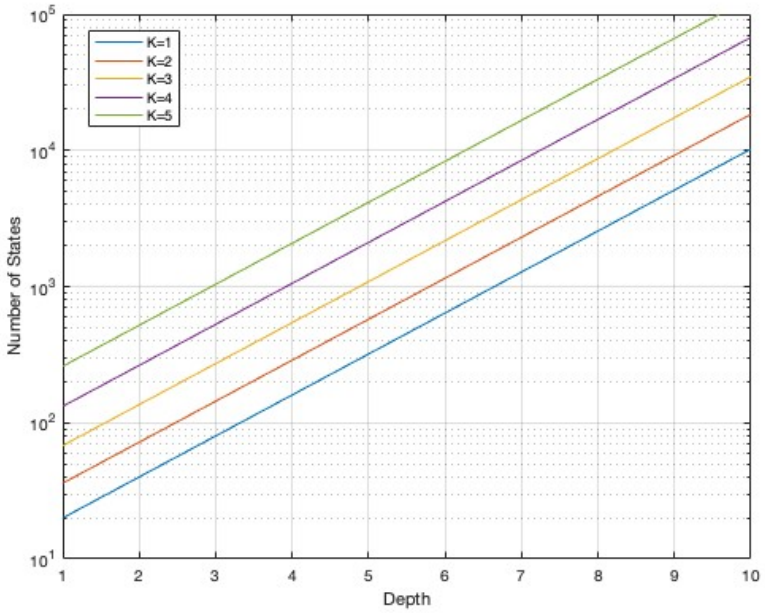


FIGURE 3.2.5: Number of States of the RExpG Tree decoder as function of both depth and k.

can be defined by the *depth* parameter, which enables the system designer to vary the complexity of the system design.

In the example of the RExpG tree decoder shown in figure 3.2.4 this presents a specific example of the tree, where the *depth* is set at a value of 1. This *depth* parameter refers to how many Unary bit states (aside from the initial Unary bit) the decoder utilises before the holding pattern is entered. This parameter can increase, which would reduce the need to monitor the 2nd and 4th bit of the RExpG codeword, but would increase the overall complexity of the receiver.

The number of Unary branches which are before the holding pattern and therefore total number of states of the RExpG tree decoder can be defined by the *depth* parameter, which enables the system designer to vary the complexity of the system design. This scaling of complexity when increasing the k and *depth* parameter, for the RExpG Tree decoder can be observed in figure 3.2.5, where the number of states can be seen increasing exponentially with depth. This increase in depth enables more unique leaf nodes and unique paths through the tree, which in turn could enable greater entropy to be achieved and potentially achieve mild performance gains.

Furthermore, figure 3.2.4 also offers an example of how the the tree decoder can be utilised to decode the symbol $d = 12$, if we trace each received bit down the binary tree, which is represented by the bold trace through the tree itself. Note, this is the same received codeword as we have shown being generated in figure 3.2.2.

Explicitly, when the first bit received is a logical 0, it is impossible for this to be a *terminal unary bit* and the trace proceeds to the right and not into the terminal FLC branch. At this point a logical one-valued bit is received for the 2nd transition, and this must be stored in memory via a counter (as it is retrieved once the decoder leaves the holding pattern). Then, at the next Unary bit, another zero-valued bit is received, and as the *depth* of this decoder is fixed at 1, the decoder enters the holding pattern. Here the 4th transition is stored in memory as a 0, and the 5th transition represents the *terminal unary bit* as a logical one-valued bit, so the decoder leaves the holding pattern and into a terminal FLC branch. As the bits for the second and fourth transition were stored in memory via the use of a counter, they enable the receiver to identify that it was symbol 12 which was transmitted by observation of a matrix which can be used to identify which symbol was transmitted. This matrix will have a width of 2^k and a depth corresponding to length of each symbol. The 'depth' of the tree, in this case where k=1, depth=1 and the codeword is 6 bits in length, this matrix has 4 rows. Specifically it is possible to identify the symbol transmitted corresponds to $d = 12$ as the second and fourth transition from the counter $'1, 0'$, with the second transition being the most significant bit. The second transition defines whether the symbol at the terminal node exists in the lower half (if it is a 1), or the upper half (if it is a 0) of all possible states. Then, the fourth transition further down selects within this half and if the codeword is longer, then the sixth, eighth and every even transition until the *terminal unary bit* can downselect until a single row is identified. The column can then be identified by the transitions in the terminal FLC tree. In this case, a 1-valued bit was transmitted which corresponds to the right-most column, and as such it is able to be identified that the symbol in location (2,3) was transmitted, corresponding to symbol $d = 12$. This is shown by the brackets in figure 3.2.4 whereby symbol 12 was able to be identified.

In comparison, in a scheme such as the ExpGEC as proposed in [142] a tree decoder would produce an infinite complexity tree, as it would be unable to generate a holding pattern as their is a variable number of bits seceding any *terminal unary bit*, which itself cannot be easily identified. This concern is visually demonstrated in figure 3.2.6, where a branch extending infinitely to the right can be observed beyond the third Unary bit. To receive additional Unary bits within the ExpG codeword, the receiver needs to expand the FLC tree sub-structure, which increases the receiver complexity exponentially. This expansion could continue up to infinity, depending on the number of Unary bits the receiver intends to receive.

In Sections 3.2.3 and 3.2.4 we introduce the finite but variable trellis used in the encoding and decoding of RExpGEC , based upon the tree discussed in Section 3.2.2.

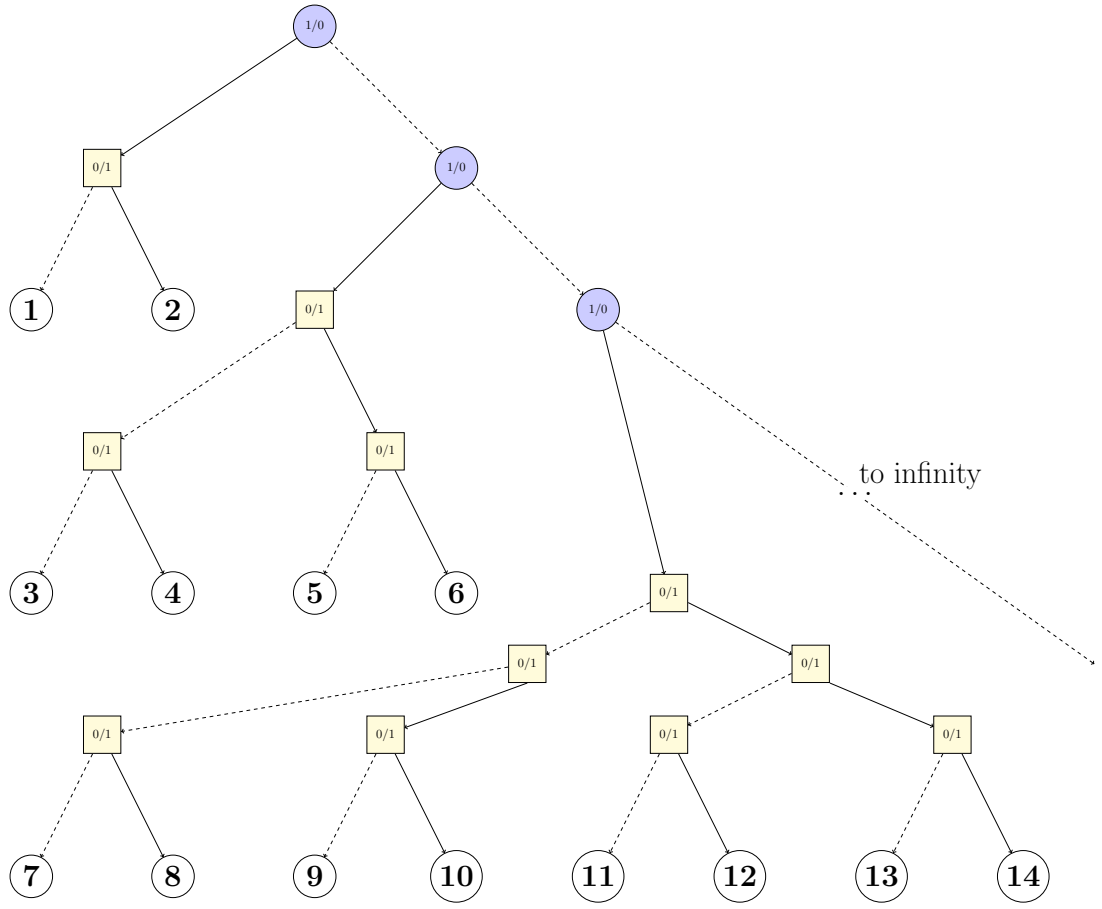


FIGURE 3.2.6: Tree Decoder for ExpG Decoder, k=1.

3.2.3 RExpGEC Trellis Encoder

In this section, we introduce the novel Trellis encoder as shown in figure 3.2.1, which in addition to the RExpG encoder creates the overall RExpGEC encoder. The RExpGEC is the JSCC generated from the base RExpG code, discussed in Section 3.2.1, via the RExpGEC trellis encoder which applies redundancy encoding according to the trellis design and codebook.

The Trellis encoder can be observed within figure 3.2.1 as a component of the overall RExpGEC encoder functionality, with the input $\mathbf{r}$ and output $\mathbf{z}$. The overall trellis structure can be observed in figure 3.2.8 and for each bit in vector $\mathbf{r}$ we progress through one stage of the trellis depending on the bit-value of the transition. The transitions that make up each individual trellis stage can be observed in figure 3.2.7 where the colour mappings of the nodes match those in figures 3.2.2, 3.2.4 and 3.2.6 to show FLC and Unary nodes with transitions between them according to the bit values in $\mathbf{r}$. Specifically, a dashed transition represents a transition occuring due to a 0 valued bit in the vector $\mathbf{r}$, and a solid transition represents a transition corresponding to a 1 valued bit in $\mathbf{r}$. Subsequently these transitions are referred to as $r_i = 0$ or $r_i = 1$.

The trellis is designed based upon the novel RExpG tree, which is discussed in Section 3.2.2, which enables a finite complexity yet flexible design to be realised for any pseudo-monotonically distributed source.

A single stage of the RExpGEC trellis, as shown in figure 3.2.7, is composed of a series of states represented as a column (m') along with a corresponding following series of states (m) and the possible transitions (m—m') between those states are indicated by a dashed line where a 0 valued bit transition occurs and a solid line when a 1 valued bit transition occurs, as mentioned above. These transitions themselves have direct mapping to the RExpG tree of figure 3.2.4. For example, node 1 of figure 3.2.4 directly relates to state 1 of figure 3.2.7 with transitions mapped accordingly to state 14 and 3 of figure 3.2.7 which are directly related to nodes 2 and 3 of figure 3.2.4. The transitions from (m—m') from each node are determined by the bit value of $\mathbf{r}$, where each transition is encoded onto a codeword, as will be described later in this section, in order to form the RExpGEC codeword associated with the vector $\mathbf{z}$ of figure 3.2.1.

The transitions can be defined according to some simple rules as follows:

- logical 1 valued RExpG transitions, where $r_i = 1$, which transit from a node n in the upper half of the trellis, complement logical 1 valued RExpG transition from node $n + 1$, where both cross the trellis.
- logical 0 valued RExpG transitions, where $r_i = 0$, which transit from a node n in the upper half of the trellis, complement logical 0 valued RExpG transition from node $n + 1$, where both transitions stay in their original half of the trellis.
- logical 1 valued RExpG transitions of the vector $\mathbf{r}$, which transit from a node where the state is a *Terminal FLC State* will immediately enter state 1 or 2, the *start/finish states*.

These transitions allow different states to be transitioned into. In order to categorise the states there are four possible types of states, which we explicitly refer to in the trellis as the following:

1. **Start/Finish States** These are the states entered at the start and end of each RExpGEC codeword, which can be entered from a Unary or a FLC transition (dependent on k), and always leave on a Unary transition. The state is between the end of one codeword and the beginning of the next.
2. **Transitory States** These are the states through which the codeword may pass for longer codewords, and they can be entered from a Unary or a FLC transition and exited on the opposite transition type to that which it was entered upon. If the exit transition is a $r_i = 1$ valued UEC transition then the remaining

transitions of the RExpGEC codeword will be FLC states, as it is a *terminal unary bit* and the trellis immediately enters either the Terminal FLC states or the *start/finish states* depending upon the value of the k parameter.

3. **Holding States** These are the states which represent the Unary and FLC states which a codeword can enter for longer RExpGEC codewords. Depending on the *depth* parameter, these holding states (which form a holding pattern) can have a higher or lower chance of being entered. If a $r_i = 1$ valued transition occurs when in the Unary holding state, it is a *terminal unary bit* and the trellis immediately enters either the Terminal FLC states or the *start/finish states* depending upon the value of the k parameter.

4. **Terminal FLC States** These states only exist where the k parameter of the RExpGEC is greater than 0, and they directly correspond to the FLC 'leaf nodes' of the RExpG tree. Once the trellis enters these states either the codeword will immediately enter the *start/finish states*, or further Terminal FLC States will be entered, dependent on the value of k.

We consider the complexity of the trellis decoder to be moderate in situations where the 'depth' parameter is low. Specifically, in the case where k=1 and depth=1 the trellis requires 140 add, compare, and select operations per iteration.

To provide an example of a specific path through the trellis, we use the RExpG codeword (d=12) = (0,1,0,0,1,1) to represent the vector $\mathbf{r}$, with state 1 being the initial state. We take the bit in the first location denoted by $r_1 = 0$, then the dashed line representing a 0 logical bit leads to state 3 (a transitory state), $r_2 = 1$ causes the transition to state 6 (a transitory state), the next location $r_3 = 0$ would take the encoder to state 10 (a holding state), $r_4 = 0$ to state 12 (a holding state), $r_5 = 1$ to state 19 (a terminal FLC state) and $r_6 = 1$ to state 2 (a start/finish state). This path is denoted as the bold path in figure 3.2.8 where several concatenated trellis stages are shown.

In order to enable a variable coding rate $\mathbf{r}$ for the RExpGEC , each transition within the trellis is assigned an output codeword of integer length $1/R$. In the case of the example shown in figure 3.2.7, $R = 0.5$ and the output of each transition is of size 2. Therefore, the symbol of $d = 12$,k= 1 which is a 6 bit vector as the RExpG codeword (as shown in figures 3.2.2 and 3.2.4) becomes a 12 bit length vector $\mathbf{z}$ as a RExpGEC codeword, of which the logical bit-values are dependent on the codebook assigned to each RExpGEC transition.

The codebook utilised for these transition must obey some rules in order to maintain maximum hamming distance between transitions when transmitted over the channel, and reduce the probability of trellis following the orthogonal path when received. These rules can be summarised as follows:

- logical $r_i = 1$ valued RExpG transitions from a node n in the upper half of the trellis, have a RExpGEC codeword output that is complement to the logical 0 valued RExpG transition from node $n + 1$.
- logical $r_i = 0$ valued RExpG transitions from a node n in the upper half of the trellis, have a RExpGEC codeword output that is complement to the logical 1 valued RExpG transition from node $n + 1$.
- logical 1 and logical 0 valued RExpG transitions from the same state must have RExpGEC codeword outputs that are orthogonal to each other.

Utilising these rules, a randomised codebook was generated to support figure 3.2.7 that produced an output vector for RExpGEC (d=12) of (1,0,1,0,0,1,1,1,0,1,1,1), which is based on the path through the trellis discussed earlier in this section.

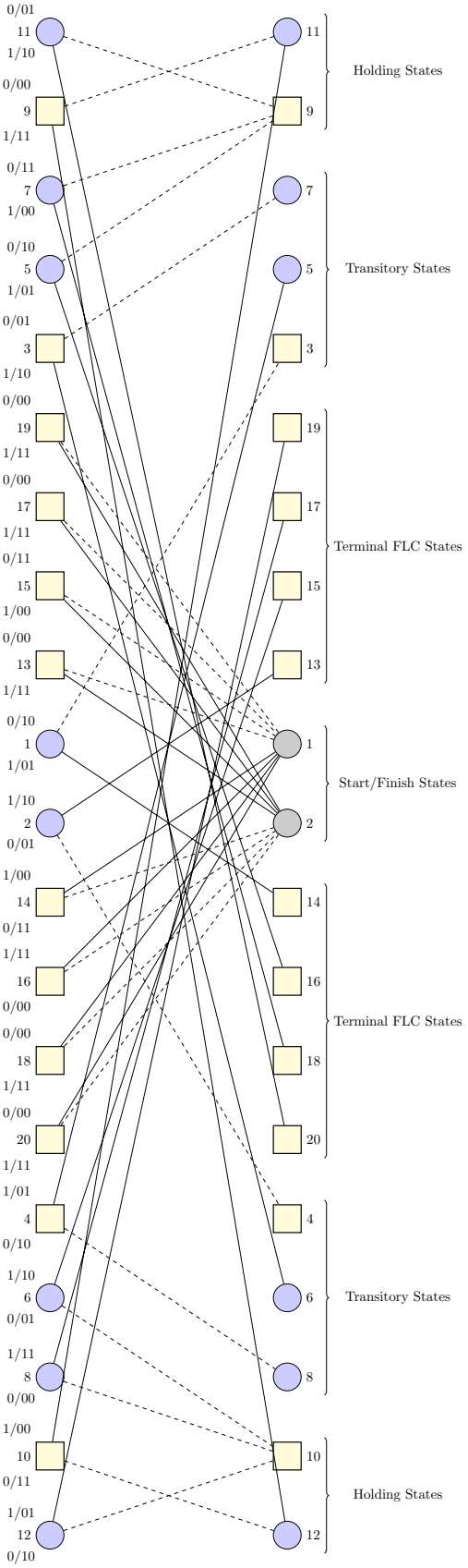


FIGURE 3.2.7: Trellis Stage for RExpGEC , depth = 1, k=1.

The trellis is mirrored and symmetrical with an upper and lower half. A state of location n in the upper half has a corresponding state $n+1$ in the lower half. For example, both state 1 and 2 of figure 3.2.7 relate to node 1 of figure 3.2.4. The reason for this mirroring is such that the trellis is designed in a manner whereby every $r_i = 1$ transition (of the RExpG code) causes a transition from the lower half of the trellis to the upper half, which allows the bit values of $\mathbf{z}$ to be equiprobable. If the RExpG was not designed to produce equiprobable bits then this would introduce capacity loss [204; 197].

3.2.4 RExpGEC Trellis Decoder

The RExpGEC decoder utilises the same trellis as that defined at the encoder. The decoder utilises the trellis to convert apriori LLRs related to encoded bits $\tilde{\mathbf{z}^{\mathbf{a}}}$, which are received from the inner decoder, into extrinsic LLRs relating to the encoded bits $\tilde{\mathbf{z}^{\mathbf{e}}}$. The decoder also outputs aposterior LLRs related to the uncoded bits $\tilde{\mathbf{r}}$ in accordance with the BCJR algorithm [205]. The BCJR algorithm [205] is a forward-backward algorithm used in digital communication for maximum a posteriori (MAP) decoding of any code that can be expressed in a trellis format. The extrinsic LLRs relating to the encoded bits $\tilde{\mathbf{z}^{\mathbf{e}}}$ can be exchanged with an inner decoder to form an iterative receiver. Within this iterative decoder the extrinsic LLRs produced by one component become the apriori LLRs to the other, with the quality of the LLRs typically improving with successive iterations. This enables iterative decoding of a series of received channel LLRs $\tilde{\mathbf{b}}$ to provide strong error correction performance.

Initially the trellis is populated with the received sequence of apriori encoded RExpGEC LLRs $\tilde{\mathbf{z}^{\mathbf{a}}}$, as well as the known probabilities of transitions $P(m|m')$ within the trellis.

The known probabilities of each trellis are calculated offline as a conditional probability from each state to the next. All initial states of the RExpGEC have 2 possible transitions from every state, corresponding to $r_i = 0$ or $r_i = 1$. In order to calculate the probabilities in an empirical manner, prior to transmission and reception, a large discrete series of symbols may be generated apriori (according to the k-parameter), which become a sequence of RExpG codewords, which are then passed into the trellis encoder, whereby each individual transition occurrence is measured and the conditional probability from each node can be calculated. Specifically, this is calculated by measuring how many times the transition corresponding to $r_i = 0$ is used in comparison to $r_i = 1$, such that from each node the $P(r_i = 1)$ transition is calculated as $No(r_i = 1)/[No(r_i = 1) + No(r_i = 0)]$ with the $P(r_i = 0)$ being $1 - P(r_i = 1)$. Following this process, and due to the RExpGEC trellis being used for both encoding and decoding, the transitions of the known conditional probabilities $P(m|m')$ of the RExpGEC trellis transitions can be calculated.

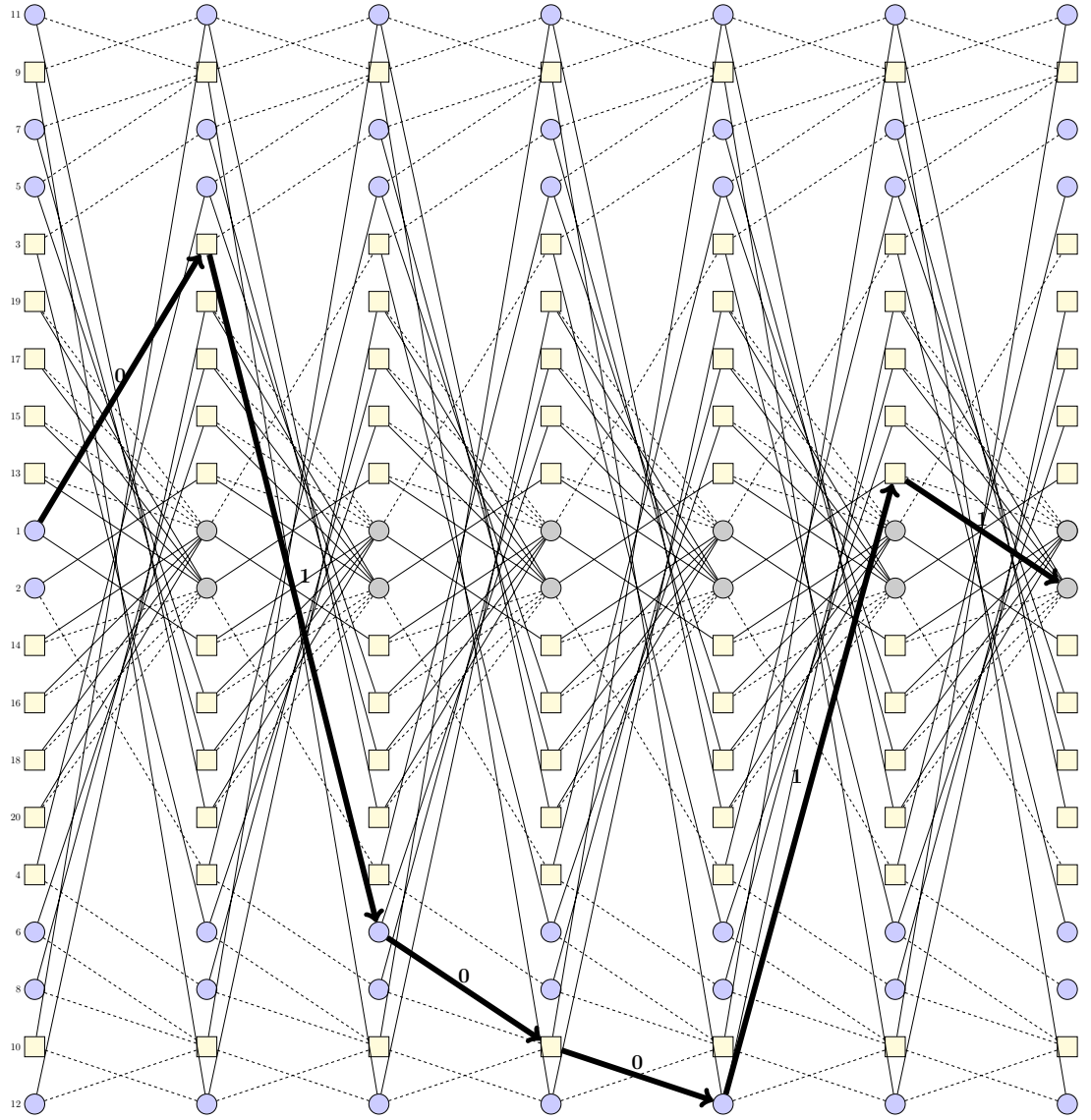


FIGURE 3.2.8: Trellis for RExpGEC , depth = 1, k=1.

The BCJR [205; 206; 140; 207] initially calculates the γ values, which are introduced in [205] which represent the probabilities of being in each state, given all the received RExpGEC apriori LLRs $\tilde{\mathbf{z}}^{\mathbf{a}}$ and the apriori known probabilities of each transition $P(m|m')$.

The algorithm then calculates the α values, which are the probabilities of reaching each state of the trellis from the previous set of states. The α values are calculated by the receiver as a function of k, *depth* of the RExpGEC and P_1 of the source and represent the likelihood of each forward transition. This forward recursion starts at the leftmost states and successively calculates α values for each set of states going from left to right [140].

Then, the algorithm calculates the backward β values, which are the probabilities of reaching each state of the trellis, given the previous state. This backward recursion

starts from the rightmost states and successively calculates β values for each set of states going to the left [207].

The BCJR algorithm combines the α, β and γ values to obtain the LLRs of each of the RExpG code bits in $\tilde{\mathbf{r}}$ [205].

Following the completion of the BCJR algorithm, a hard decision can be made on all aposterior LLRs of the encoded bits to realise the vector $\hat{\mathbf{x}}$ as per figure 3.2.1. This is done by analysing the sign of LLRs in $\tilde{\mathbf{r}}$, where postive LLRs represent a binary 1 and negative a binary 0. If the codewords are correctly received and the iterative code is able to correctly converge then these bits should directly match the RExpG codewords for the transmitted symbols $\boldsymbol{x}$, as discussed in Section 3.2.1 and in Section 3.2.2.

3.3 System Design

In this section, we present a novel system design which exemplifies the proposed JSCC RExpGEC code. This system concatenates the RExpGEC as introduced in Section 3.2 with a URC [208] and QPSK modulation [105; 133; 134]. The system is henceforth referred to as the RExpGEC-URC-QPSK scheme. The system design introduces the key aspects of the RExpGEC scheme to achieve a balance between flexibility and performance. The key components of the system are thoroughly discussed in this section to provide a clear understanding of the system, including the constituent code components. This section serves as a cornerstone for the evaluation of the system's performance, which is presented in subsequent sections of the chapter.

In Section 3.3.1 we introduce the block diagram of the system. Section 3.3.2 introduces the system parameters and how they will be used in subsequent analysis.

EXIT chart analysis of the RExpGEC-URC-QPSK scheme is provided in Section 3.3.3, and for comparison with a comparable SSCC in Section 3.4. Furthermore, comparison with a JSCC benchmarker, the REGEC code of [106] can be made utilising the specific example of $k = 0$, as the underlying REGEC can be seen as a special case of the RExpGEC where $k = 0$.

3.3.1 System Model

The RExpGEC-URC-QPSK system is presented in the block diagram in figure 3.3.1, where a vector of symbols $\mathbf{x}$ is generated, which are turned into a vector of RExpG uncoded bits $\mathbf{r}$ and subsequently RExpGEC encoded bits $\mathbf{z}$. These RExpGEC encoded bits are interleaved with Π_1 to form $\mathbf{a}$, then encoded with a URC code to produce encoded RExpGEC-URC bits $\mathbf{y}$. The RExpGEC-URC bits are then interleaved with Π_2 into the vector $\mathbf{b}$ and mapped to QPSK modulation for transmission over a

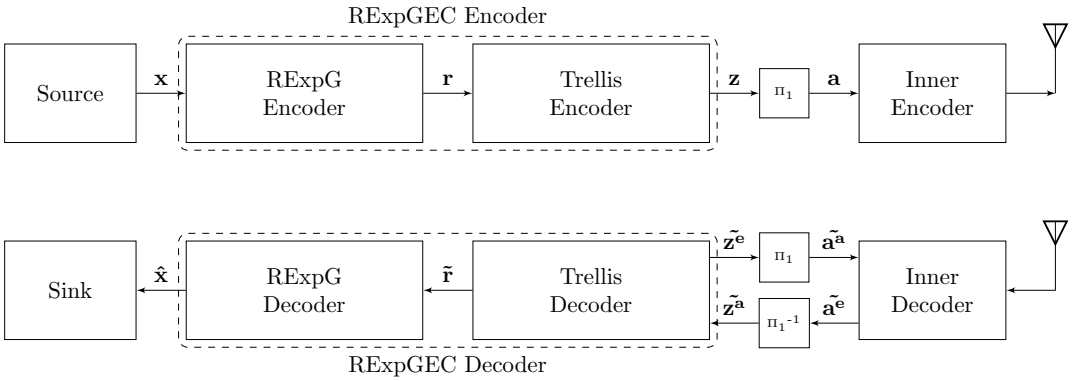


FIGURE 3.3.1: Block Diagram for RExpGEC with URC2 and QPSK Mapping.

wireless channel. For the receiver the signal is received, demapped according to the QPSK demapper, interleaved encoded LLRs corresponding to the URC encoded signal $\tilde{\mathbf{b}}$ and the interleaver π_2^{-1} are deinterleaved to form $\tilde{y}$. These LLRs then undergo the first operation of the URC decoding to form the extrinsic LLRs from the URC decoder $\tilde{\mathbf{z}^{\mathbf{a}}}$, along with a zero-valued $\tilde{a^a}$ (apriori information from the RExpGEC decoder). Following this the RExpGEC Trellis is populated with $\tilde{\mathbf{z}^{\mathbf{a}}}$ and iterative decoding between the RExpGEC Trellis decoder and URC decoder commences, where the output $\tilde{\mathbf{z}^{\mathbf{e}}}$ becomes the input to the URC of $\tilde{a^a}$ when interleaved with Π_1 and the output of the URC $\tilde{a^e}$ becomes the input to the RExpGEC $\tilde{\mathbf{z}^{\mathbf{e}}}$ when deinterleaved with π_1^{-1}. When the iteration limit is reached or the system has converged, a decision is made on the uncoded RExpG LLRs $\tilde{\mathbf{r}}$ and the received symbols $\hat{\mathbf{x}}$ is provided to the Sink.

For the inner code, the URC is chosen in order to harness the iterative performance of turbo-style receivers whilst incurring moderate coding complexity [209]. The URC coding rate has a rate exactly equal to 1, such that the number of bits at the output $\mathbf{y}$ is exactly equal to the bits at the input $\mathbf{a}$, yet it introduces recursion into the bitstream, such that the bits depend upon each other. This then enables iteration and iterative information gain. URC codes have been proposed for a wide variety of diverse applications for such iterative purposes [210; 211; 212; 213] and are well suited as an inner code for the RExpGEC-URC-QPSK scheme. Therefore, the incorporation of a carefully designed URC enables flexible iterative coding design when used as an inner code for moderate complexity gain and no change to the overall RExpGEC coding rate. The complexity of the RExpGEC-URC-QPSK when the RExpGEC trellis decoder is concatenated with the URC code produces 154 add, compare, and select operations per iteration in the specific case of k=1 and depth=1, however it is acknowledged that this complexity will increase for differing k and depth parameters.

3.3.2 Simulation Parameters

In order to analyse the performance of the RExpGEC and further enhance the scheme design, a number of simulation parameters require to be chosen for undertaking initial EXIT chart analysis [214; 215] and then in turn Symbol Error Rate performance, in comparison to the JSCC and SSCC benchmarker.

The variables which are chosen by the system designer are as follows:

- **k Parameter** The k parameter of the RExpGEC code will be set at different values for analysis of various options, specifically 0,1, and 2, in order to remain consistent with examples shown in Section 3.2. The k parameter controls the length of the FLC bits at the end of the codeword, as shown in Table 3.2.1. A higher k value better matches a flatter source distribution with a lower P_1.
- **Coding Rate** The coding rate R_o of the RExpGEC can be altered by varying the bits allocated to each RExpGEC trellis transition as discussed in Section 3.2.3. In order to remain consistent with prior work [106] for comparison the coding rate R_o for the benchmarker will be set at $1/2$.
- **Trellis 'Depth'** The trellis depth will affect the complexity of both the encoder and decoder, which is discussed in Section 3.2.2. In order to remain consistent with examples shown in Section 3.2 the trellis depth will be set at a value of 1.
- **URC States** The URC operates on the basis of a trellis that uses the BCJR algorithm and we can control the number of states in it. However for consistence with prior work [106] two-state URC shall be used.
- **Modulation Mapping** The modulation mapping scheme chosen is required to be consitent across all benchmarkers. In order to remain consistent with prior work [106], QPSK shall be used.

The variables dependent on the zeta-distributed source include:

- P_1 **of Source:** P_1 represents the probability of the first symbol in any source distribution. The characterisation of a zeta-like (or geometric) distributed source involves its size and P_1 value. Various information sources exhibit variable P_1 values, typically falling within the range of 0.5 - 0.75, as discussed in [142]. This chapter presents results for P_1 values ranging from 0.1 to 0.9.
- **Finite Source Size:** For simulation purposes, a finite source size needs to be chosen. In our case, a symbol dictionary size of $L = 1000$ is selected for the simulations presented in this work, maintaining consistency with prior research [106].

Parametric analysis on the depth parameter has shown that the truncation gained from having a shorter depth has minimal impact on performance for source dictionaries when $L = 1000$. Through inspection of the transitions of lower stages in the tree it can be observed that even for large and infinite cardinality sources a transition is rarely observed. As these lower stages are where the gain would be expected, a larger depth has little overall performance gain. However, if a receiver has a large computational power, a system designer may still choose to implement a higher 'depth' parameter to observe good performance from the RExpGEC component code. Furthermore, EXIT chart analysis shows that the EXIT charts presented in Section 3.3.3 for a depth of 1 are indistinguishable from those with higher depths.

For simulations we use a fading channel with Rayleigh distribution in our simulations, and present performance results as a function of E_b/N_0 (which enables a direct comparison between different source distributions and their respective information entropies).

3.3.3 EXIT Chart Analysis

Within this section, we conduct detailed analysis on the iterative nature of the RExpGEC-URC-QPSK scheme and estimate its performance using EXIT chart analysis [105; 216; 174] to gain an enhanced understanding of the transfer of information between the component codes of the RExpGEC-URC-QPSK scheme. The EXIT charts are presented in figures 3.3.2 to 3.3.4. The quality of the information being transferred between the RExpGEC and URC component codes is quantified via the measurement of the mutual information [146] of the LLR values being passed between the component codes and their corresponding bit values from the transmitter. We analyse the mutual information at $\tilde{\mathbf{z}^{\mathbf{a}}}$ referred to as I_a and that of $\tilde{\mathbf{z}^{\mathbf{e}}}$ referred to as I_e, which represents the apriori and extrinsic information to and from the RExpGEC component code. This enables an enhanced understanding of how the mutual information of the LLRs increases in an iterative manner.

EXIT functions represent the iterative performance gain that can be achieved by a component code of an iterative scheme, as such the present the mutual information of the LLRs as a function of the quality of the extrinsic information as a function of the quality of the apriori information which is presented to the code.

In this section, EXIT functions of both the RExpGEC and URC will be presented on the same axes in order to represent how information will iterate between the RExpGEC and URC codes. It is important to note that RExpGEC functions are inverted EXIT functions, as the extrinsic information I_e becomes the apriori information I_a of the URC code.

Therefore, in order to visualise the 'EXIT tunnel'[149] of the RExpGEC-URC-QPSK scheme they are presented in this manner, the URC EXIT functions are not inverted due to the URC code being the inner code, thus the apriori LLRs to the URC are the apriori LLRs for the overall RExpGEC-URC-QPSK scheme.

The transformation of I_a into I_e by the trellis decoder of figure 3.3.1 is characterised by plotting the inverted RExpGEC EXIT function in an EXIT chart [216], as shown in figures 3.3.2 to 3.3.4. In this case the inverted RExpGEC EXIT curve reaches the (1, 1) point in the top right corner of the EXIT chart [217]. Since the URC decoder also has an EXIT curve that reaches the (1, 1) point in the top right corner of the EXIT chart [149] as shown in figures 3.3.2 to 3.3.4, iterative decoding convergence towards the Maximum Likelihood (ML) performance of the RExpGEC-URC-QPSK scheme is facilitated [218; 219].

The RExpGEC-URC-QPSK scheme may be said to operate near-capacity operation if reliable communication can be maintained at transmission throughputs that approach the CCMC capacity C [134] that is associated with $M = 4$ QPSK modulation in an uncorrelated Rayleigh fading channel. Previous work on EXIT charts [204] have shown that the proposed scheme will offer near capacity performance if the the URC decoder of figures 3.3.2 to 3.3.4 has an EXIT curve with an area beneath it of $A^i = C/[R_o log_2(M)]$ and the area A^o beneath the inverted EXIT curve of the RExpGEC trellis decoder in figures 3.3.2 to 3.3.4 approaches the RExpGEC coding rate R_o.

If these two conditions are satisfied, then near-capacity operation will be achieved, when the shape of URC decoder's EXIT curve is closely matched to that of the inverted RExpGEC EXIT curve. This creates a narrow, but marginally open EXIT chart tunnel, which facilitates iterative decoding convergence. This narrow EXIT tunnel can be observed in figures 3.3.2 to 3.3.4, where the EXIT tunnels are characterised for various values of k.

These EXIT tunnels provide an indication of when the RExpGEC-URC-QPSK scheme will start to converge, as can be observed in the SER plots, the scheme fully converges with signal power levels approximately 1 dB larger than the point at which the EXIT tunnel opens.

The EXIT chart area A_o that is situated below the inverted RExpGEC EXIT curve is given by [198; 204; 106]

$$A_o = \frac{1}{n} \sum_{m'=1}^{r} \sum_{m=1}^{r} P(m|m') log_2(\frac{1}{P(m|m')}), \tag{3.5}$$

where $P(m|m')$ represents the probability of a transition within the decoder, and $\mathbf{r}$ is the maximum number of states within the decoder.

In figures 3.3.2 to 3.3.4 the EXIT function of the URC and the inverted EXIT function of the RExpGEC are shown for a given SNR when the EXIT tunnel is first presented

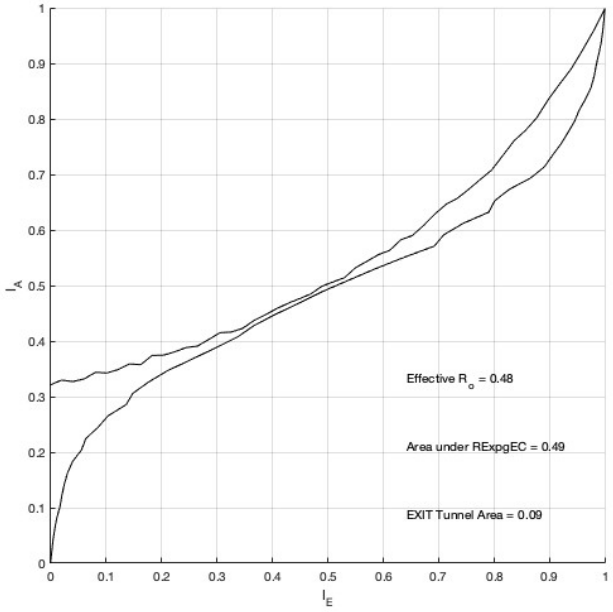


FIGURE 3.3.2: EXIT chart demonstrating the EXIT tunnel opening parameters for $k = 0$ for the inverted RExpGEC EXIT function against the corresponding URC EXIT function at variable E_b/N_0, $P_1 = 0.6$, block length = 10000, $L = 1000$, SNR = 0.9 dB, CCMC capacity = -0.4 dB.

as open. At this point, the RExpGEC-URC-QPSK scheme should be expected to start to converge [219]. It is important to note that the RExpGEC code with a k parameter of 0, as shown in figure 3.3.2 is a special case of the RExpGEC that enables the RExpGEC to be functionally equivalent to the REGEC code presented in [106]. Therefore, this can be viewed as a benchmarker for a JSCC in comparison to the RExpGEC component code of the RExpGEC-URC-QPSK scheme.

As shown in figures 3.3.2 to 3.3.4, the A_o approaches the effective coding rate R_o of the RExpGEC at the value of $P_1 = 0.6$. This shows that the 2-state URC code choice of [106] also offers near optimal performance in the RExpGEC-URC-QPSK scheme.

The EXIT analysis shows that the URC choice of the two state URC for the RExpGEC-URC-QPSK scheme is a good match for near-capacity performance and demonstrates efficiency in its design. The EXIT charts also provide a strong indication of the potential performance of a ML decoder for the proposed RExpGEC-URC-QPSK scheme which will be further explored via simulation in the following section.

3.4 Results and Analysis

In this section, we characterise the Symbol Error Rate performance of the RExpGEC-URC-QPSK scheme and compare it with two benchmarker schemes. The

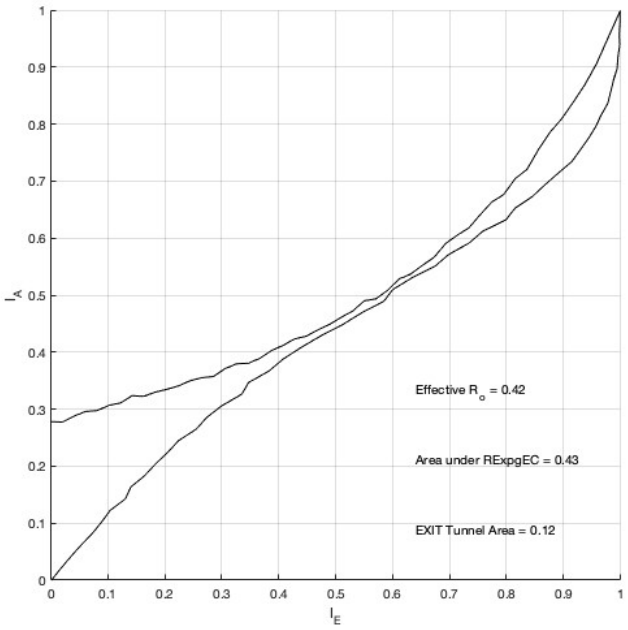


FIGURE 3.3.3: EXIT charts demonstrating the EXIT tunnel opening parameters for $k = 1$ for the inverted RExpGEC EXIT function against the corresponding URC EXIT function at variable E_b/N_0, $P_1 = 0.6$, block length = 10000, $L = 1000$, SNR = 0.4 dB, CCMC capacity = -0.1 dB.

first benchmarker scheme is a SSCC scheme which uses the ExpG code concatenated with a convolutional and URC channel codes and then QPSK modulated. The second benchmarker is the REGEC-URC-QPSK scheme from [106], which represents a special case of the RExpGEC-URC-QPSK scheme where k=0 is the only supported parameter value. We will show that our proposed RExpGEC-URC-QPSK scheme offers superior performance in comparison to both the SSCC and JSCC benchmarker both in terms of absolute near-capacity performance, but also in flexibility of design, specifically the ability to match different source distributions more efficiently in comparison to the REGEC-URC-QPSK benchmarker.

In the ExpG-CC-URC-QPSK scheme shown in figure 3.4.1, the source symbol vector $\mathbf{x}$ is encoded into a ExpG bit vector, which is encoded with a convolutional code [129] interleaved via π_1 and encoded with an URC encoder (of the same code rates as that used in the RExpGEC-URC-QPSK scheme) to produce a vector of ExpG-CC-URC bits $\mathbf{y}$, and then mapped to QPSK modulation for transmission. This enables a direct comparison with the RExpGEC-URC-QPSK scheme as the ExpG-CC-URC-QPSK scheme is the SSCC equivalent.

The ExpG-CC-URC-QPSK benchmarker scheme will observe the same coding rate R_o as the RExpGEC-URC-QPSK scheme as introduced in figure 3.3.1. Furthermore, as the ExpG-CC-URC-QPSK scheme is based upon the Exponential Golomb codeword, it can be scaled to different values of k for direct comparison with the

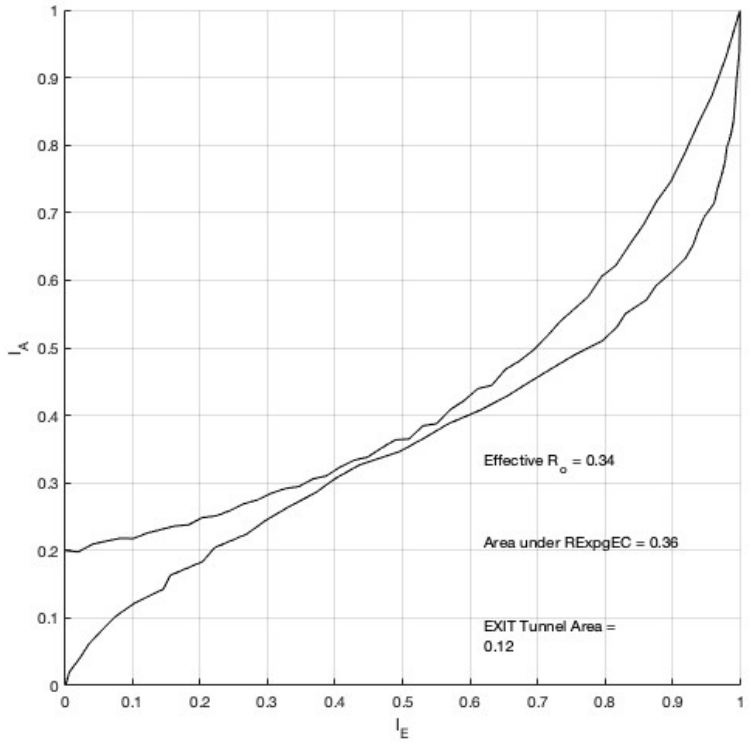


FIGURE 3.3.4: EXIT charts demonstrating the EXIT tunnel opening parameters for $k = 2$ for the inverted RExpGEC EXIT function against the corresponding URC EXIT function at variable E_b/N_0, $P_1 = 0.6$, block length = 10000, $L = 1000$, SNR = 0.6 dB, CCMC capacity = 0.1 dB.

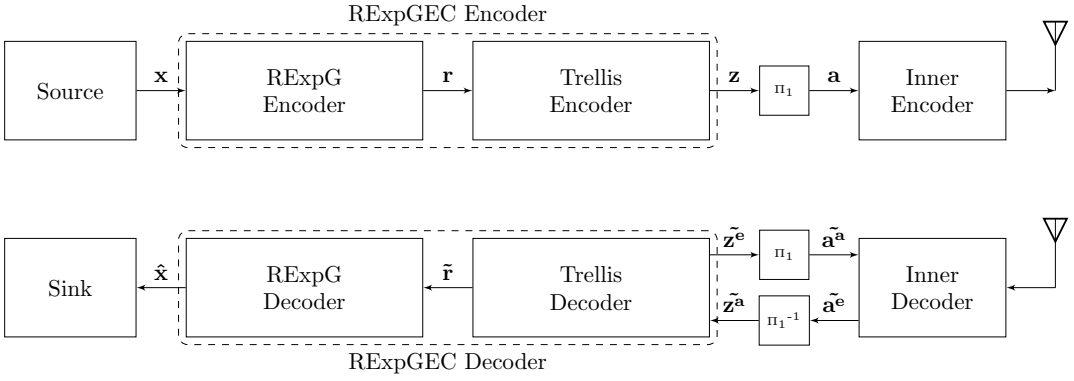


FIGURE 3.4.1: ExpG-CC-URC-QPSK Block Diagram.

RExpGEC-URC-QPSK scheme for the values of k which are simulated. The complexity of the ExpG-CC-URC-QPSK benchmarker scheme is relatively modest in comparison with the 154 add, compare, and select operations per iteration of the RExpGEC-URC-QPSK (where k=1 and depth=1), with a fixed complexity of 42 add, compare, and select operations per iteration. This is due to the fixed decoder structure of the SSCC scheme, where the decoder does not vary with k. Specifically in the case where k=1 and depth=1, the RExpGEC-URC-QPSK scheme is 3.6 times more complex than the ExpG-CC-URC-QPSK benchmarker scheme.

In order to evaluate the performance of the RExpGEC-URC-QPSK scheme in comparison with the ExpG-CC-URC-QPSK scheme, simulations were conducted using well motivated values of P_1, k, and L, which are the same as those discussed in Section 3.3.2 whereby the performance of both systems can be directly compared. Specifically 100 iterations were applied to all schemes, with early termination criteria applied if the vector $\hat{\mathbf{x}}$ matched the transmitted symbol vector $\mathbf{x}$.

Figure 3.4.2 characterises the performance of the RExpGEC-URC-QPSK scheme introduced in Section 3.3 in figure 3.3.1, and provides direct comparison with the benchmarker ExpG-CC-URC-QPSK scheme introduced in Section 3.4 in figure 3.4.1. The scenario shown in figure 3.4.2 is one snapshot of a series of simulation parameters, with other results presented in figures 3.4.3 and 3.4.4.

As shown in figure 3.4.2, reliable transmission can be achieved for zeta distributed sources with a P_1 of 0.6 at 1.7 dB for $k = 0$, 1.9 dB for $k = 1$, and 2.2 dB for $k = 2$. This performance constantly outperforms the benchmarker SSCC scheme and is constantly within 2.1 dB of the CCMC capacity for this specific case. Note, CCMC capacity of differing k parameters varies due to the different operating spectral efficiencies with regards to E_b/N_0.

As can be seen in figure 3.4.2 the RExpGEC-URC-QPSK scheme is close to capacity for these specific cases. In figures 3.4.3 and 3.4.4, the results from several different parameter values are presented, specifically including results on the variation of P_1 and k, with performance shown in both E_b/N_0 as well as channel SNR.

The values used to produce these plots can also be observed in Table 3.4.1.

The parametric performance of the RExpGEC-URC-QPSK and ExpG-CC-URC-QPSK schemes with respect to P_1 with performance measured in E_b/N_0 and SNR are presented in figures 3.4.3 and 3.4.4, respectively. As can be observed in figure 3.4.3 the performance of the RExpGEC-URC-QPSK outperforms the ExpG-CC-URC-QPSK SSCC benchmarker for all cases with regards to E_b/N_0 across various P_1, and offers similar performance for all k parameters, which includes the JSCC benchmarker of the REGEC-URC-QPSK. The gap to CCMC capacity does not exceed 2.73 dB for any scenario and in the vast majority of cases is below 2 dB.

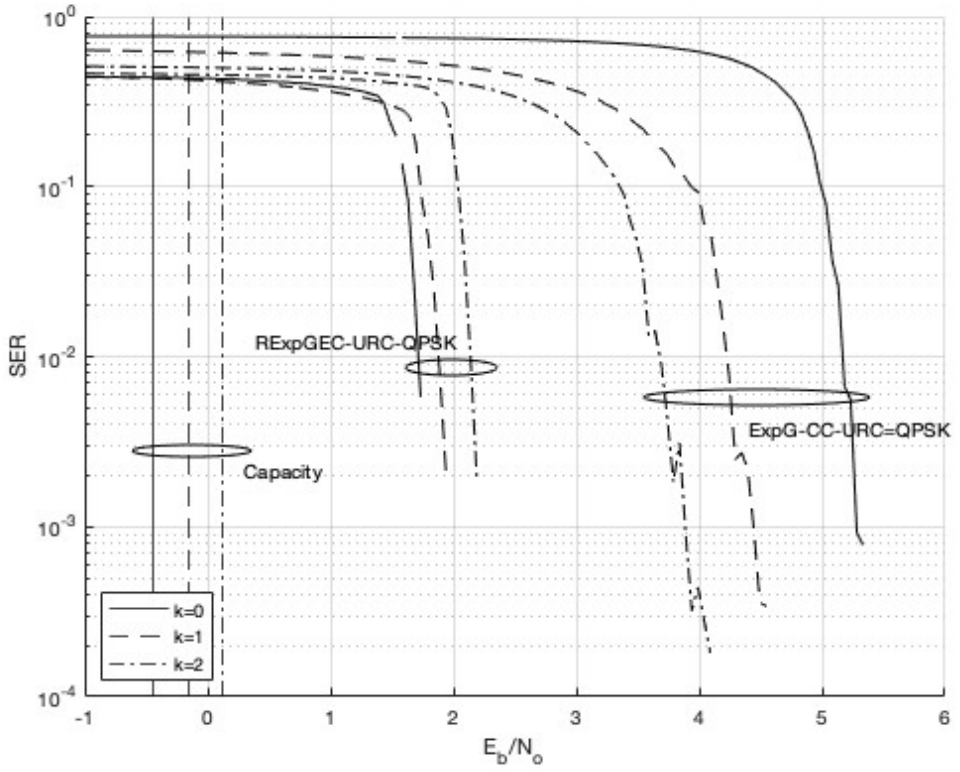


FIGURE 3.4.2: Symbol Error rate of the RExpGEC-URC-QPSK and ExpG-CC-URC-QPSK, for variable k parameters with block length = 10000, P_1 of 0.6, and $L = 1000$.

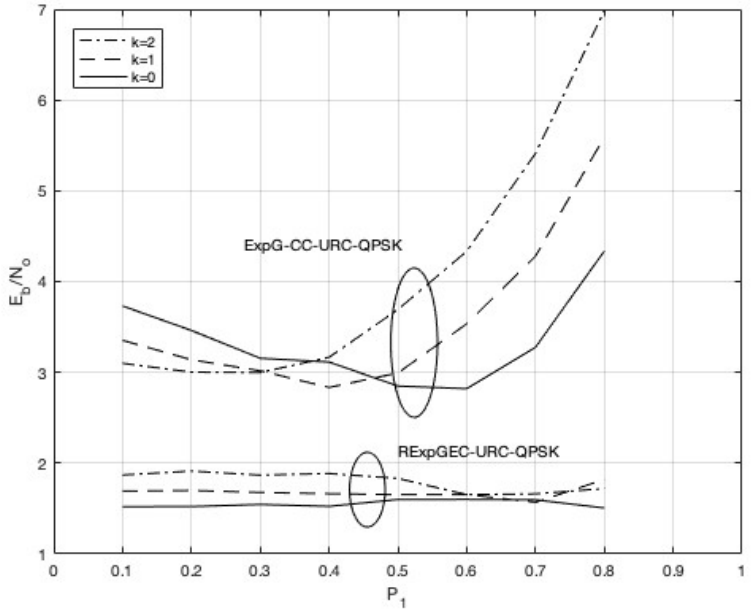


FIGURE 3.4.3: E_b/N_0 of the RExpGEC-URC-QPSK and ExpG-CC-URC-QPSK, for variable P_1 parameters with block length = 10000, $L = 1000$, and $k = 0,1,2$.

P_1	Scheme	k	Spectral Efficiency (bits/s/Hz)	CCMC Capacity (dB)	E_b/N_0 (dB)	Gap to Capacity (dB)	SNR (dB)
0.1	ExpG-CC	0	0.83	-0.17	3.73	3.90	2.94
0.2	ExpG-CC	0	0.88	-0.08	3.46	3.55	2.89
0.3	ExpG-CC	0	0.92	0.01	3.16	3.14	2.80
0.4	ExpG-CC	0	0.96	0.10	3.11	3.02	2.94
0.5	ExpG-CC	0	0.98	0.14	2.85	2.71	2.77
0.6	ExpG-CC	0	0.97	0.11	2.82	2.71	2.68
0.7	ExpG-CC	0	0.90	-0.03	3.28	3.31	2.82
0.8	ExpG-CC	0	0.76	-0.32	4.34	4.66	3.12
0.1	RExpGEC	0	0.83	-0.17	1.52	1.69	0.73
0.2	RExpGEC	0	0.88	-0.08	1.52	1.61	0.95
0.3	RExpGEC	0	0.92	0.01	1.55	1.53	1.19
0.4	RExpGEC	0	0.96	0.10	1.52	1.43	1.35
0.5	RExpGEC	0	0.98	0.14	1.60	1.46	1.52
0.6	RExpGEC	0	0.97	0.11	1.60	1.49	1.46
0.7	RExpGEC	0	0.90	-0.03	1.60	1.63	1.14
0.8	RExpGEC	0	0.76	-0.32	1.51	1.83	0.29
0.1	RExpGEC	1	0.88	-0.06	1.69	1.76	1.15
0.2	RExpGEC	1	0.92	0.01	1.70	1.69	1.33
0.3	RExpGEC	1	0.95	0.07	1.68	1.61	1.44
0.1	ExpG-CC	1	0.88	-0.06	3.35	3.42	2.81
0.2	ExpG-CC	1	0.92	0.01	3.14	3.13	2.77
0.3	ExpG-CC	1	0.95	0.07	3.02	2.95	2.78
0.4	ExpG-CC	1	0.95	0.08	2.83	2.75	2.63
0.5	ExpG-CC	1	0.92	0.02	2.99	2.97	2.65
0.6	ExpG-CC	1	0.84	-0.15	3.53	3.68	2.79
0.7	ExpG-CC	1	0.71	-0.42	4.28	4.70	2.77
0.8	ExpG-CC	1	0.52	-0.76	5.59	6.35	2.77
0.4	RExpGEC	1	0.95	0.08	1.66	1.58	1.46
0.5	RExpGEC	1	0.92	0.02	1.65	1.63	1.31
0.6	RExpGEC	1	0.84	-0.15	1.65	1.80	0.91
0.7	RExpGEC	1	0.71	-0.42	1.57	1.99	0.06
0.8	RExpGEC	1	0.52	-0.76	1.82	2.58	-1.00
0.1	RExpGEC	2	0.92	0.01	1.87	1.86	1.49
0.2	RExpGEC	2	0.93	0.04	1.91	1.87	1.62
0.3	RExpGEC	2	0.93	0.04	1.87	1.83	1.57
0.4	RExpGEC	2	0.90	-0.04	1.89	1.92	1.42
0.5	RExpGEC	2	0.82	-0.20	1.83	2.03	0.96
0.1	ExpG-CC	2	0.92	0.01	3.10	3.09	2.72
0.2	ExpG-CC	2	0.93	0.04	3.00	2.96	2.71
0.3	ExpG-CC	2	0.93	0.04	3.00	2.96	2.70
0.4	ExpG-CC	2	0.90	-0.04	3.17	3.20	2.70
0.5	ExpG-CC	2	0.82	-0.20	3.69	3.89	2.82
0.6	ExpG-CC	2	0.69	-0.44	4.33	4.77	2.75
0.7	ExpG-CC	2	0.54	-0.73	5.41	6.14	2.75
0.8	ExpG-CC	2	0.38	-1.01	6.98	7.99	2.73
0.6	RExpGEC	2	0.69	-0.44	1.65	2.09	0.07
0.7	RExpGEC	2	0.54	-0.73	1.66	2.39	-1.00
0.8	RExpGEC	2	0.38	-1.01	1.72	2.73	-2.53

TABLE 3.4.1: Performance metrics of the RExpGEC-URC-QPSK scheme in comparison to the ExpG-CC-URC-QPSK, including the gap to CCMC capacity for a given Spectral Efficiency (which itself is a product of η, Modulation Order and Code Rate)

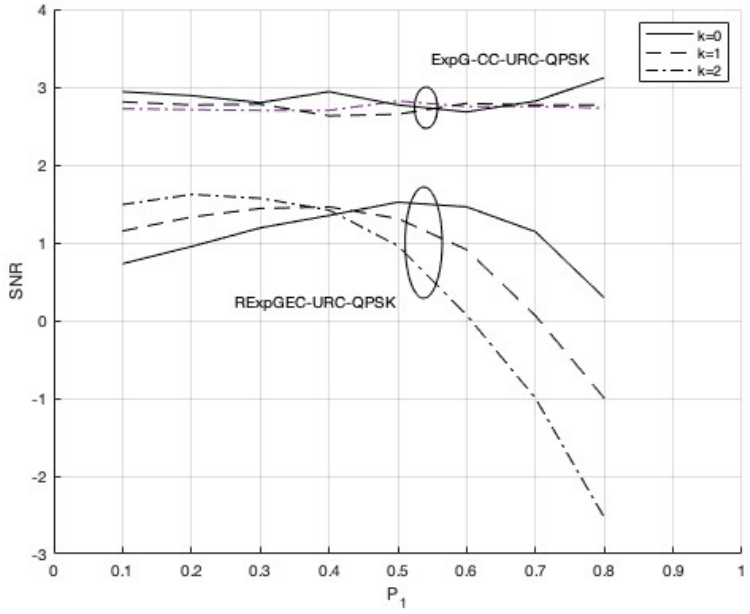


FIGURE 3.4.4: SNR of the RExpGEC-URC-QPSK and ExpG-CC-URC-QPSK, for variable P_1 parameters with block length = 10000, $L = 1000$, and $k = 0,1,2$.

In comparison for link-budget constrained deployments where SNR is the important performance metric the results shown in figure 3.4.4 are relevant. In this case not only does the RExpGEC-URC-QPSK still outperform the SSCC benchmarker but dependant on P_1 it can also offer better performance than the REGEC-URC-QPSK JSCC benchmarker. This demonstrates the flexibility of the RExpGEC-URC-QPSK. In all cases, all RExpGEC-URC-QPSK schemes with varying k outperforms all ExpG-CC-URC-QPSK by at least 1 dB.

The relationship between SNR and E_b/N_0 is characterised by equation Eq. (3.6) below, where η is the information efficiency described previously, R_o is the coding rate of the convolutional code and M is the modulation order.

$$E_b/N_0(dB) = \text{SNR}(dB) - 10\log_{10}(\eta) \times R_o \times log_2(M) \tag{3.6}$$

In these cases, the flexibility of the RExpGEC-URC-QPSK scheme offers significant benefit over the REGEC-URC-QPSK scheme of [106], which can be functionally seen as a special case of the RExpGEC-URC-QPSK scheme where k=0, due to the fact that the system can be designed to utilise a different k parameter, and have better SNR performance. This is particularly useful if the system designed is constrained by the link budget, whilst maintaining a tight energy efficiency criteria as the system maintains a similar energy efficiency in terms of energy per bit for all values of k and P_1, whereas the SNR performance varies and the system can be optimised accordingly.

3.5 Chapter Conclusion

In this chapter, we have introduced a novel JSCC code, known as the RExpGEC , which when integrated into the novel RExpGEC-URC-QPSK scheme provides near-capacity transmission of symbol values that are selected from large or infinite monotonic source distributions.

The RExpGEC-URC-QPSK scheme has enhanced flexibility over its JSCC counterpart such as the REGEC-URC-QPSK scheme, whilst maintaining the same performance level for k=0. The RExpGEC-URC-QPSK scheme enables enhanced performance for other values of the k parameter and maintains a gap to the CCMC capacity of 2 dB for all values of P_1 for zeta-like source probability distributions, when QPSK modulation is employed for transmission over an uncorrelated narrowband Rayleigh fading channel.

In some practical scenarios where the source symbols obey particular finite Zeta-like source probability distributions, our RExpGEC-URC-QSPK scheme is shown to offer gains of up to 3.6 dB over SSCC benchmarkers in all cases, when QPSK modulation is employed for transmission over an uncorrelated narrowband Rayleigh fading channel.

These gains are achieved for no-cost with regards to spectral usage and power, without increasing the required transmit-duration, transmit-bandwidth or transmit-energy. However, this is achieved at the cost of complexity of around 3.6 times compared to the SSCC benchmarker when k=1 and depth=1. We consider these performance gains to be significant, since they are achieved within the vicinity of the CCMC capacity, namely within 2 dB. This is achieved by mitigating the capacity loss inherent in SSCC, which is due to the residual redundancy after source coding which is not exploited for error correction. Furthermore the gains are achieved by being able to adjust the k parameter to target different monotonic sources in link-budget constrained scenrios. Since these gains are associated with the improvements offered by the RExpGEC code over the benchmarker SSCC and JSCC codes, similar gains may be expected when combining with any other channel codes.

Within the following chapter on LLR based signal processing for tactical communications, the EXIT chart approaches discussed within this chapter on physical layer performance prediction is further explored, specifically in the activity regarding the sub-block turbo equalizer for continuous phase modulation scheme waveforms. Whereby the performance of the novel sub-block turbo equalizer undergoes EXIT chart analysis prior to simulation in a Rayleigh fading channel.

Chapter 4 : LLR Based Signal Processing for Tactical Communications

In this chapter, we embark on an exploration of LLR based signal processing for tactical communications with the aim of enhancing the efficacy of tactical communications. Our journey takes us through various approaches, where we delve into innovative strategies for demodulating M-ary orthogonal signalling, to improve robust spread spectrum communications. Additionally, we introduce a novel turbo equalizer specifically designed for seamless integration with Continuous Phase Modulation schemes, exemplified within the NATO Narrowband waveform.

Chapter 4 can be seen within the structure of the overall thesis in figure 4.1.1.

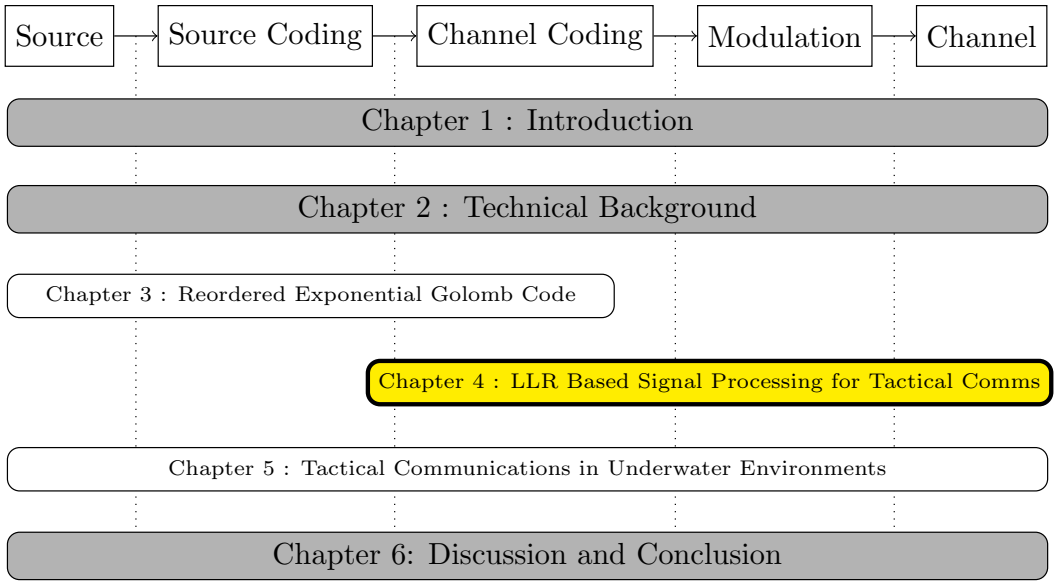


FIGURE 4.1.1: Structure of the Thesis

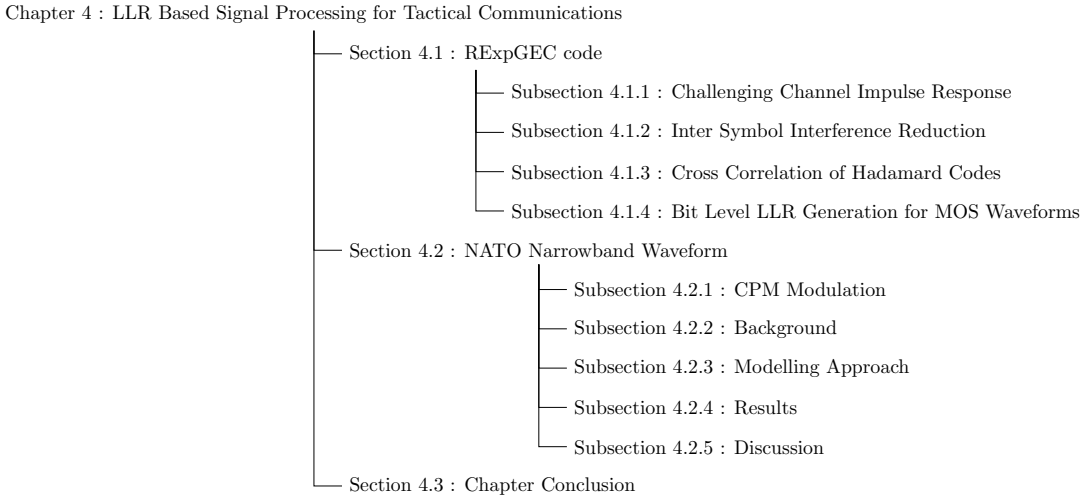


FIGURE 4.1.2: Structure of Chapter 4

Figure 4.1.1 highlights that Chapter 4 explores the areas of channel coding, modulation and channel specifics.

This chapter introduces pioneering techniques that revolutionise the generation of bit-level LLR) within tactical environments, enabling flexible soft decoding of bit-level channel coding schemes. In the initial section, a novel approach to the demodulation of M-ary Orthogonal Signalling is presented. In contrast to current methods [109] that compromise performance by relying on hard-decision approaches to obtain bit-level values, the outlined novel techniques eliminate this limitation, potentially enhancing performance by 2 or 3dB. Additionally, the chapter emphasises a novel equalisation approach specifically tailored for challenging environments, customised for differentially encoded modulation schemes. The efficacy of this scheme is evaluated in Rayleigh fading channels [110], simulating tactical urban deployment scenarios [111]. The assessment reveals noteworthy improvements, especially in scenarios characterised by rapid phase inversions, such as those encountered by helicopters in deployment scenarios where traditional equalizers [112] may falter. This chapter signifies a substantial advancement in overcoming practical challenges in wireless communication, particularly in complex and dynamic deployment environments.

The overall structure of this chapter is presented in figure 4.1.2 which provides the reader with a high level overview of the work discussed within this chapter.

Aspects of Chapter 4 have been published in [8] and solely represents the author of this thesis contributions, it is important to note the author of this thesis was the lead researcher of the published paper, however due to the paper being published after their tenure at Dstl, Joe Kellett who was at Dstl at the time of publication was the primary author for submission due to requirements of the publication processes within UK government.

4.1 M-Ary Othogonal Signalling

Section 4.1 introduces the novel concept of M-ary Orthogonal Signalling for use in communications in challenging multi-path channels, as a form of modulation to enable reasonable data rate communications in multi-path limited environments.

Further in the thesis, Chapter 5 introduces a specific use of M-ary Orthogonal Signalling in Underwater Acoustic communications channels, which will be used to support underwater and autonomous operations. Within Section 5.5 this link between underwater communications and autonomy is explored further.

4.1.1 Challenging Channel Impulse Response

Within this section, we will introduce a particularly challenging channel used to stress and provide system parameters to aid the design of the M-ary Orthogonal Signalling, specifically in this case the focus will be on underwater acoustic channels, which will be further explored within this thesis in Chapter 5.

Underwater Acoustic Channels typically have delay spreads of upwards of 50 ms with second or third order paths of comparable magnitude arriving up to 150 ms after the original reception [116; 3; 2]. Perhaps an even more challenging characteristic is that due to deep ocean acoustic channels, sometimes earlier arrivals may be weak and suffer phase non-linearities due to being the surface path with the final received signal being the strongest and most coherent [6; 220; 115].

Typically Underwater Acoustic communications cope with this adverse channel through the use of increasing Bandwidth Time (BT) product of the waveforms through spreading codes with good auto-correlation properties to average the detection over a longer time or wider bandwidth, such as those used in Direct Sequence Spread Spectrum (DSSS) codes [221; 222]. Should these codes have good cross-correlation properties they also have the advantage of being able to offer code division multiple access schemes to reduce inter-node interference and to enable low-overhead addressing through multi-cast,uni-cast and broadcast addressing.

An underwater communications system may be afforded 10 kHz of bandwidth [223; 224; 225], when operating with a carrier frequency above 40 kHz this carrier bandwidth provides a 0.1 ms bit period for standard BPSK. Therefore within a typical multi-path of 50ms there are 500 bit periods which could be affected by significant Inter Symbol Interference (ISI), requiring a much larger equalizer than that used typically in RF communications where multipath may be a few bit periods.

This disparity between typical RF channels where multipath causes ISI of the order of a few bit periods, compared to underwater acoustics where a sparse channel will cause

ISI of a large number of bit periods motivates a different approach to modulation scheme design for underwater acoustic communications.

Further, this causes different motivations for utilising spread spectrum, whereas in the RF domain spread spectrum techniques would typically be used for link budget and power optimisation, whereby the gain from spreading enhances the amount of energy that can be used to transmit a single bit of information, whereas in the underwater domain this spreading is predominantly used to aggregate energy to reduce the impact of the sparse multipath channel, instead of increasing the link budge performance.

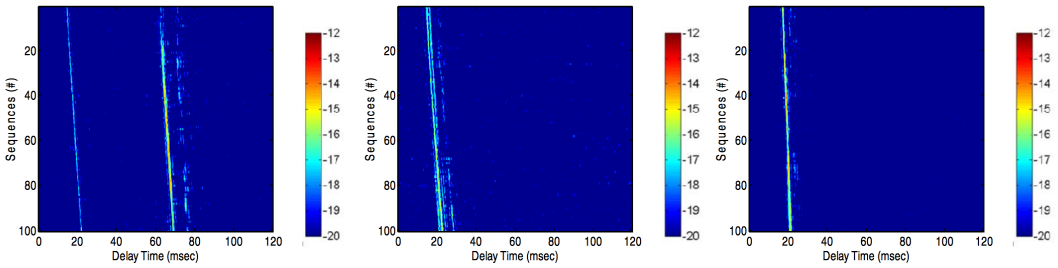


FIGURE 4.1.3: Channel Impulse responses of an example sparse underwater acoustic channel (in relatively deep waters) off the east coast of Taiwan. From [223]

An example of the channel impulse response of a typical shallow water underwater acoustic channel can be observed in figure 4.1.3, taken from [226] showing delay spreads up to 80ms, suggesting that in order to reduce ISI a symbol duration of 80ms must be used, in [226] the transmit carrier frequency of 5 kHz was used with a bandwidth of 2 kHz. This corresponds to 0.5 ms per bit period. With these channel parameters and in order to cope with 80ms of time delay spread a chip with a Bandwidth-Time (BT) product of *80(ms)/0.5(ns) = 160* must be used, see eq. Eq. (4.1). In the case of [226] m-sequences [227] were chosen with a BT product of 511, corresponding to chip time of *511/0.5(ms) = 255.5(ms)*; thereby providing enough BT product to overcome severe channel reverberation when using a matched filter on the receiver.

$$\text{Minimum BT Product Required} = \frac{\text{Time Duration of Impulse Response}}{\text{Symbol Duration}} \tag{4.1}$$

4.1.2 Inter symbol Interference Reduction in Challenging Channels

In severe multipath channels, there exists several methods for being able to reduce ISI between respective symbols, either in multi-carrier communications or single-carrier communications. In this chapter the focus will be on developing a novel a Direct Sequence Spread Spectrum (DSSS) like approach, known as M-ary Orthogonal Signalling, in order to cope with the multipath of an challenging communications channel.

Typically DSSS spectrum communication schemes spread the energy of a transmitted bit over a Pseudo-Noise (PN) code of length BT (known as the bandwidth time product), however in turn this directly corresponds to a data-rate loss of exactly BT as the signal is being reduced in data transmission terms by this length of spreading code.

However it is also known that for most PN code sets, such as m-sequences [228] or Q-Phase codes [229] there exists not just 2 codes (one allocated to bit 0 and one allocated to bit 1) but often there are BT number of PN codes that can be sent.

Therefore, through utilisation of many different PN codes of the same length, with reasonable cross-correlation properties it is possible to conduct the novel approach to M-ary Orthogonal signalling, whereby each transmitted PN code (symbol) corresponds directly to a number of binary bits. The number of information bits that can be transmitted corresponds directly to $Log_2(M)$.

In order to ensure that we have maximum performance orthogonality and thus spectral efficiency, it is important that a code family is chosen that has good orthogonality in its cross-correlation performance; therefore the Walsh-Hadamard code was chosen, as it has perfect cross-correlation properties, as to say that at the zero-lag cross correlation all Walsh-Hadamard codes are orthogonal. The properties of these codes are explored further in Section 4.1.3.

In Section 4.1.3 the properties of Walsh-Hadamard codes is discussed further, and in Section 4.1.4 more details will be discussed on how bit level LLRs can be obtained to allow for flexible channel coding schemes, and packet sizes. However in practice with the Phorcys protocol suite a combination of the Walsh-Hadamard code modulo a Q-Phase is used at a Physical layer to achieve optimal communications performance, this is due to the poor auto-correlation properties of the Walsh-Hadamard codeword set. In practice this combination allowed for a good combination of cross-correlation (for MAry Orthogonal Signalling) and auto-correlation (for multi-path performance).

4.1.3 Cross Correlation of Hadamard Codes

In order to achieve bandwidth efficient communications as discussed in Section 4.1.2 it is possible to use the near-perfect cross-correlation properties of the Walsh-Hadamard codes generated from the Hadamard matrix.

These codes when presented through the cross-correlation function present a zero-output for all codewords other than the intended codeword at a lag of 0. This is represented for the case when the length of the Hadamard code is equal to 64 in figure 4.1.4 which represents the cross-correlation function of Hadamard code 1, figure 4.1.5 which represents the cross-correlation function of Hadamard code 2, and figure 4.1.6 which represents the cross-correlation function of Hadamard code 3 with

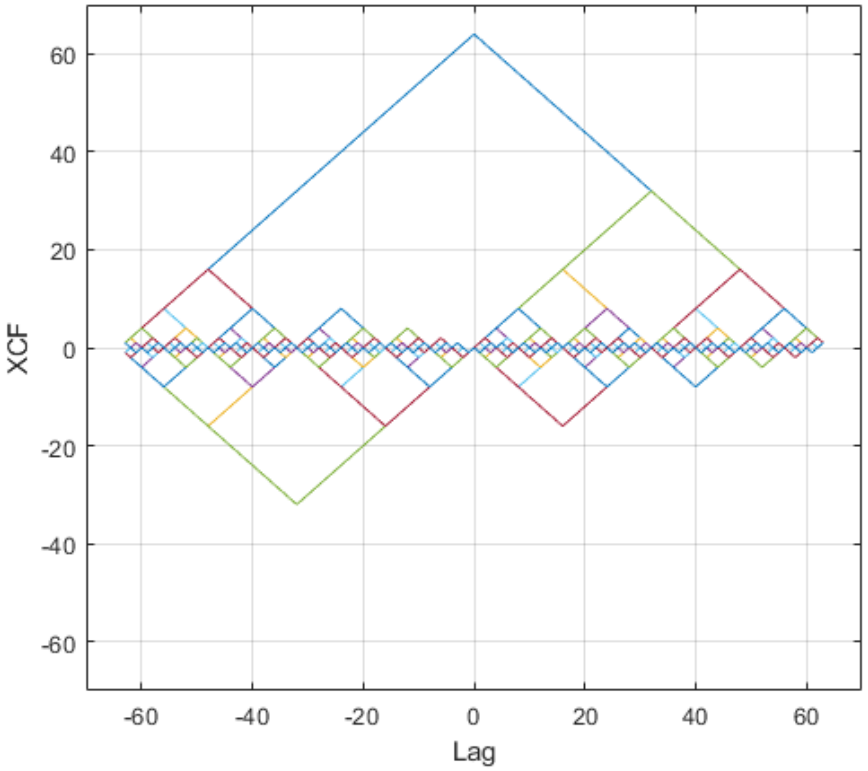


FIGURE 4.1.4: Cross-Correlation Function of Hadamard Codeword 1 with all Hadamard Codes for $M = 64$

all other Hadamard codewords of length 64. These cross-correlation functions are presented in the absence of any noise.

These cross-correlation functions have been chosen to demonstrate how the cross correlation can vary across all possible Hadamard codes of length 64. For example in figure 4.1.4 whilst the auto-correlation of Hadamard code 1 is extremely poor, with a near linear roll-off, any lag in the codeword would likely not reduce the performance significantly as no other codeword has a close cross correlation with this codeword. Due to the poor auto-correlation this would not be suitable for timing alignment.

Comparatively with codeword 2 in figure 4.1.5 it can be observed that there is an auto-correlation peak when the lag is 0, but this has alternating peaks with various lags, and similar to codeword 1 has no close correlation with other Hadamard codes.

However, due to the low autocorrelation with a small lag and alternating peaks this codeword may have poor performance if timing is not aligned. Not, due to these multiple peaks this codeword could not be used for timing alignment itself.

In comparison to codewords 1 and 2, codeword 3 highlights the need to have good timing alignment for systems utilising Hadamard codes for their cross-correlation properties. In the case of codeword 3 as can be seen in figure 4.1.6 if there is any lag at

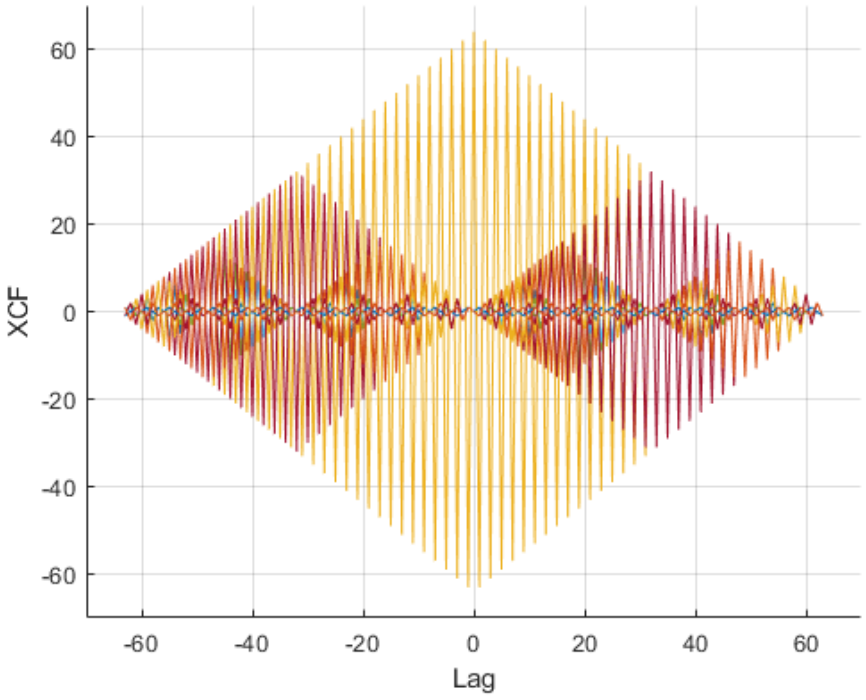


FIGURE 4.1.5: Cross-Correlation Function of Hadamard Codeword 2 with all Hadamard Codes for $M = 64$

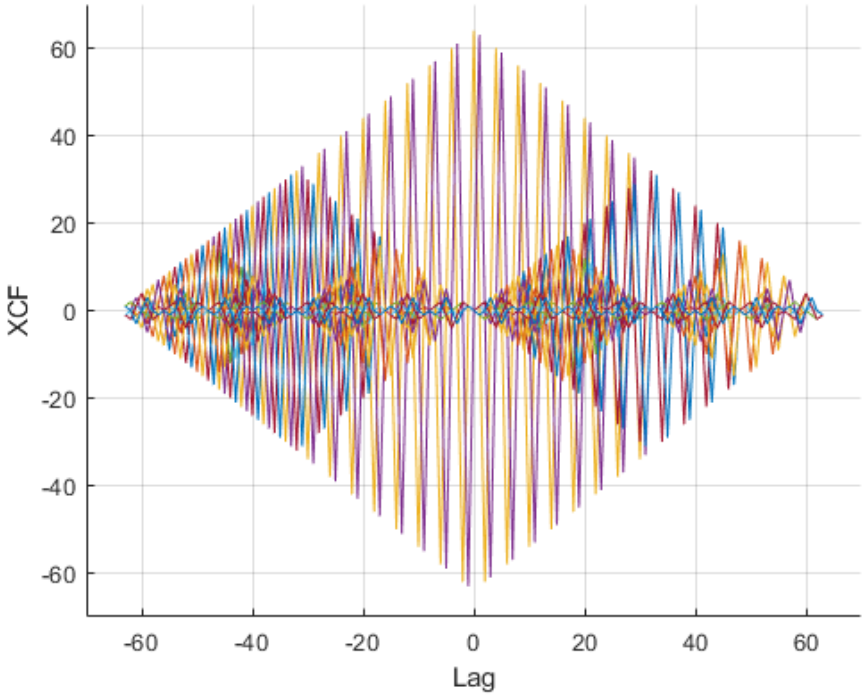


FIGURE 4.1.6: Cross-Correlation Function of Hadamard Codeword 3 with all Hadamard Codes for $M = 64$

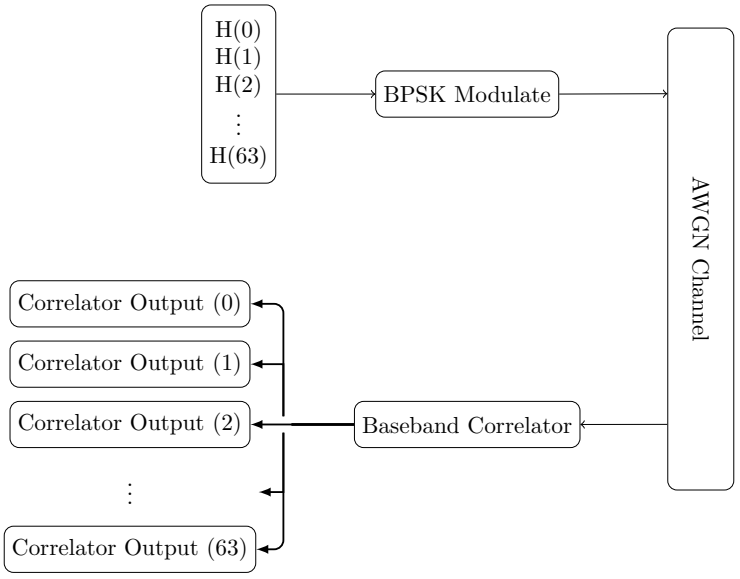


FIGURE 4.1.7: Block diagram of the simulation

all due to a timing misalignment there is a peak in cross-correlation for another codeword that is offset by only 1 bit.

This cross-correlation concern and lag alignment motivates the need to have strong timing alignment for the practical deployment of Hadamard codes for transmission of information.

Moreover, when in the presence of noise these codes no longer exhibit perfect orthogonality, therefore one must take an approach to recover the original intended Hadamard code; through the use of a correlator, similar to that used in CDMA schemes [230]. The correlator would require to search over all possible codewords in order to generate a magnitude response of the predicted received codeword.

In turn this Hadamard code must be mapped back to bitwise LLRs to allow for decoding with a binary channel coding scheme. However the correlator will provide confidence outputs for each individual correlator of the set, which exist as independent correlator values.

For simulation a model has been generated in MATLAB that modulated Hadamard codewords with BPSK modulation over an AWGN channel. On the receive side a baseband correlator was used with an assumption that the receiver was in perfect synchronisation with the transmitter. This approach is designed in collaboration with the non-coherent transmission used in the simulated system. A block diagram of this model can be seen in figure 4.1.7

This model allowed for observation of the statistics of the output of each correlator. A histogram of the correlator statistics can be observed in figure 4.1.8, these statistics

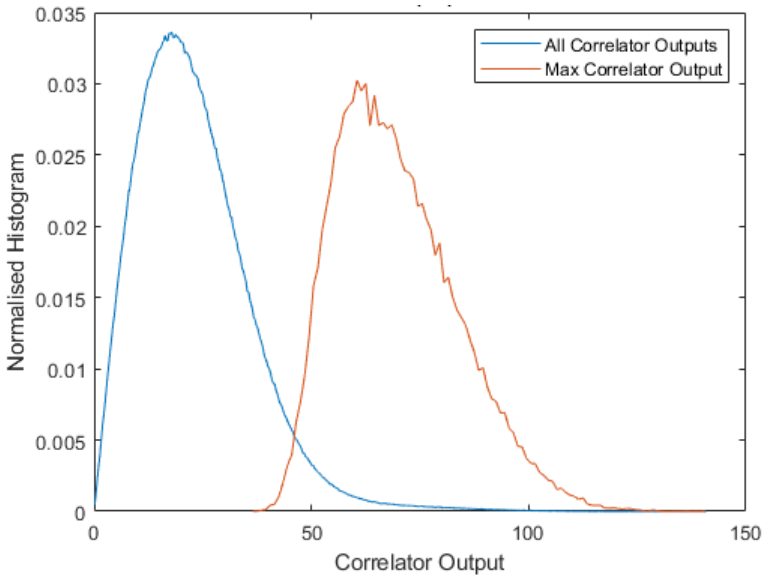


FIGURE 4.1.8: Histogram of Correlator Outputs of Hadamard Code for $M = 64$ at -10 dB SNR

were gathered from the transmission and reception of 1,000,000 Hadamard codewords of length 64 with an Additative White Gaussian Noise (AWGN) SNR of -10 dB. This SNR is measured at the chip level, such that it is at the output of the channel rather than at the output of the Hadamard correlators.

4.1.4 Bit Level LLR Generation for MOS

Following on from the block diagram in figure 4.1.7, and as discussed in Section 4.1.2, we would wish to transmit $log_2(M)$ bits of information within one codeword where $M = BT$ in the case of the Hadamard M-ary orthogonal signalling.

In order to facilitate soft LLR binary channel coding schemes, such as those discussed in Chapter 2 we must be able to gain appropriate bit level LLRs from the output of the correlator.

Assigning bit mapping to these codewords allow for optimised performance in multipath channels, whilst negating some of the aspects of data throughput reduction which is caused via spread spectrum in the time domain.

As mentioned each correlator output exists as an independent parameter which is variable in accordance with the channel noise, and auto-correlation function of a given codeword out of an overall set of 64 possible combinations (in the case of $M = 64$).

The correlator outputs can be considered as a function of the likelihood that the correct codeword has been received givern all possible transmitted codewords and of the channel itself; therefore one approach could be to try to undertake a method to

estimate the channel and remove the effects from the received signal completely in order to keep this as purely a function of the transmitted codeword, but in low signal to noise ratios this would have poor performance.

Another method would be to compare the observe the statistics of the overall correlator magnitude output, and to treat this as the 'noise' signal, effectively removing the mean value of this output, leaving one outlier to provide likelihood ratios for the remaining correlator output magnitudes.

Then much like in standard LLR generation whereby we scale the LLR by the output of the noise, it is possible can create a look up table whereby each correlator output is scaled by σ^2, in order to create a noise scaled LLR, this pragmatic approach allows symbol level LLRs to be created in accordance with each codeword.

Once symbol level LLRs are generated it is possible to generate bitwise LLRs, once again, there are many ways to conduct this stage; however as the LLRs are already in the logarithmic domain it is possible to take the maximum magnitude symbol level LLR and from a look up table for the M bits which this represents assign the sign of the bits respectively in order to create bit level LLRs.

A simple method would be to take a hard decision, which would ultimately result in performance loss, another soft decision approach is presented in [231], however the author proposes a novel approach to achieve bitwise LLRs from a soft output receiver to have optimal decoding performance from M-ary Orthogonal signalling schemes.

The proposed approach utilises the property of natural binary mapping for each M-ary codeword, such that for each bit position it can be identified which MOS symbols this would map to, and then a bit level LLR can be generated for this known bit location using the Eq. (4.2). To provide an example, in the case of the first bit location for a M=64 case, the first 32 symbols (0-31) contain a '0' at bit location 1 whilst the remaining symbols contain (32-63) contain a '1' at bit location 1. In Eq. (4.2) B_i refers to the 'bit index' for the calculated LLR, where the max term indicates the maximum value of the correlator output for either where the 'bit index' refers to a 0 or 1 mapping; the sum term refers to the average of all possible MOS symbols which could be the opposite bit value. The equation is derived from Eq. (2.8) which provides a bit level LLR given the known probability of a received bit.

$$\mathrm{LLR}_{\mathrm{MOS}}(B_i) = \frac{\max\left[\text{Corr Output}(B_i = 1)\right]}{\sum\left[\text{Corr Output}(B_i = 0)/M\right]} - \frac{\max\left[\text{Corr Output}(B_i = 0)\right]}{\sum\left[\text{Corr Output}(B_i = 1)/M\right]} \quad (4.2)$$

In order to validate whether the LLRs are correctly being scaled we can measure the expected value of the LLRs against the true values that are being received, the approach as described shows that this relationship although linear has a scaling error,

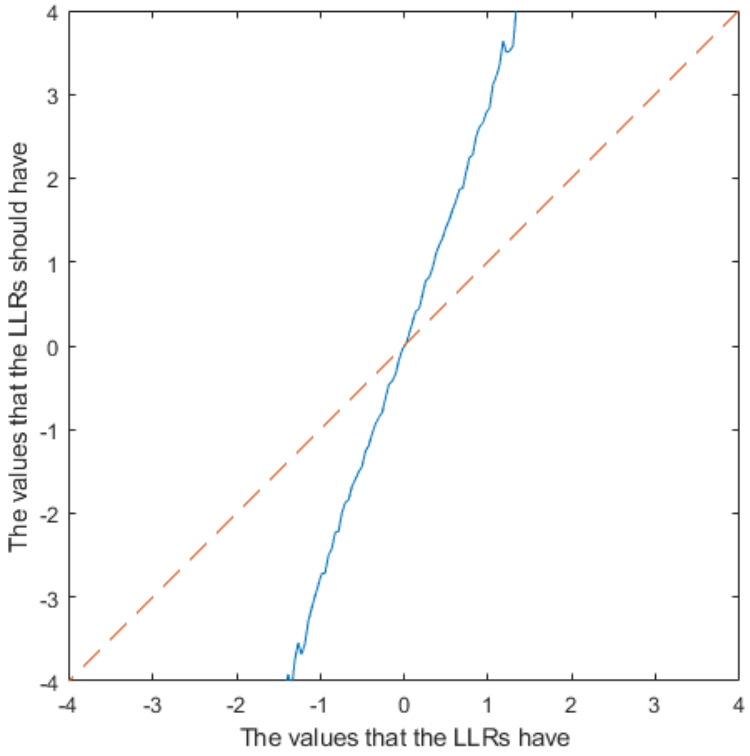


FIGURE 4.1.9: Scaling of LLRs against input Bits at SNR = -10 dB

as can be seen in figure 4.1.9. This scaling factor can significantly affect channel coding schemes that are sensitive to scaling LLRs such as LDPC codes utilising the Sum-Product approximation in variable and check nodes.

Another method to assess the quality of the output LLRs is to view the histogram of the output LLRs, as can be seen in figure 4.1.10.

Using this approach it is possible to measure the Mutual Information of the LLRs, the method used to measure the Mutual Information is described in Chapter 2 and can be used to understand whether the output bit level LLRs can be utilised to achieve good channel code performance.

The SNR dependent mutual information of multiple M-OS schemes can be seen in figure 4.1.11, by measuring the mutual information of the received LLRs it is possible to confirm that indeed the LLRs are performing the function as expected, it is also able to observe and use these as a planning tool for channel coding design.

As can be seen in figure 4.1.11 for each increase in M we get approximately 5dB performance gain in an AWGN environment.

This comparison may not be fair in terms of energy, however in this work the emphasis is on overall link budget performance, whereby operation at low channel SNR is a critical design constraint.

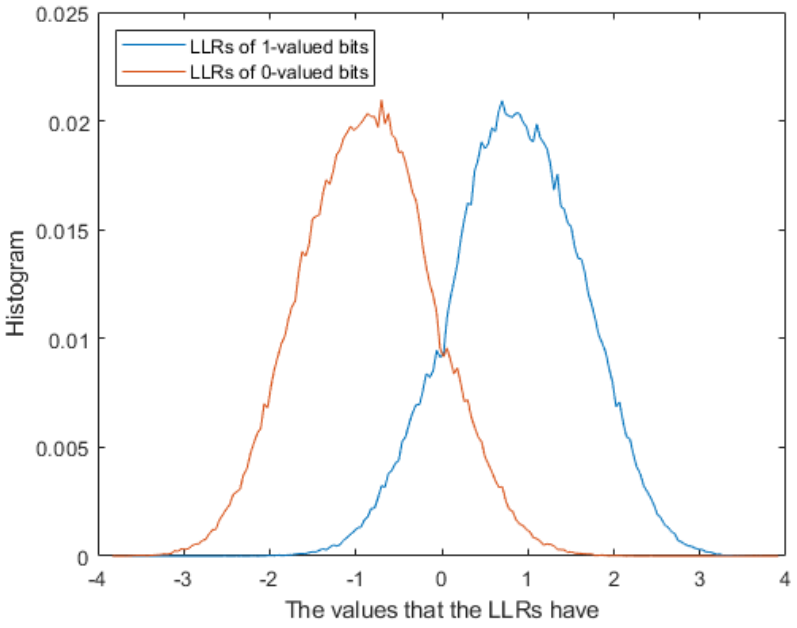


FIGURE 4.1.10: Histogram of LLRs for $M = 64$ at SNR = -10 dB

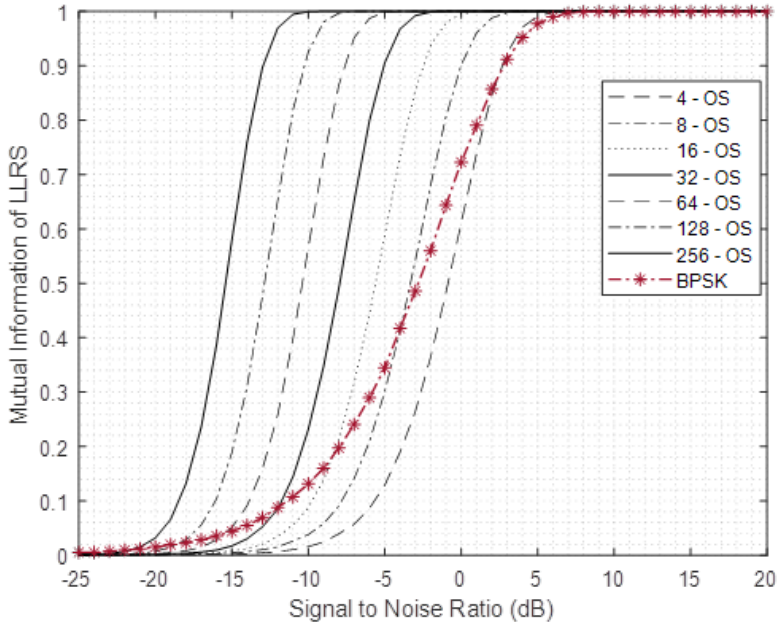


FIGURE 4.1.11: Mutual Information of bit-level LLRs of varying M-OS

This gain in increase of M provides enhanced performance predominantly due to the increase in length of the underlying Hadamard code, and as such aggregated power over that codeword.

These bit-level LLRs enable for more granularity on the channel coding to be utilised which maintaining optimal performance. This is in contrast to the symbol level probabilities used in [6], and would enable more flexibility to be employed with channel coding rate.

To conclude this section the intricacies of underwater acoustic channels, characterised by substantial delay spreads from multipath conditions, demand specialised considerations in the design of communication systems. M-ary Orthogonal Signalling, particularly through the use of Walsh-Hadamard codes, emerges as a promising solution to mitigate the challenges presented by the underwater environment whilst maintaining a reasonable data throughput. This section has shown the complexities of the underwater channel and the rationale behind adopting MOS techniques to effectively address these challenges.

Within the next section we will continue the introduction of novel techniques for LLR-based signal processing for tactical communications, as a novel turbo-equalizer is proposed for a NATO wireless communications standard, whereby the traditional full-block turbo equalizer may offer poor performance in highly spread channels.

4.2 NATO Narrowband Waveform

This section introduces a novel sub-block turbo-equalizer for the NATO Narrowband waveform [104], which produces LLRs which can then be used in the decoding process to improve the performance of the demodulator of a NBWF communications transmission to be 1.1 dB from CCMC capacity, this is done for a complexity that is 2 times as complex as the full block turbo equalizer.

The NBWF is a VHF/UHF communications protocol that provides tactical communications for dismounted and mounted operations across a variety of operating environments. It is important to note this is in contrast to the environment discussed in the earlier part of Chapter 4, which is aimed at the underwater acoustic channel.

4.2.1 CPM Modulation Waveform

Continuous Phase Modulation (CPM) schemes are used in a wide variety of NATO interoperability standards, most notably the NATO Narrowband Waveform (AComP 5631) [104], Common Data Link (STANAG 7085) [158] and Very Low Frequency (VLF) Communications (STANAG 5030) [159].

The NATO Narrowband Waveform (NBWF)[104] aims to achieve interoperability between coalitions at a tactical level. It aims to provide performance improvements over its predecessors through the implementation of a continuous phase modulation scheme in conjunction with channel coding in the form of convolution code.

In this section we analyse the performance of the physical layer of the NBWF N1 mode [104] in various channels and introduce the idea of a sub-block turbo equalizer to improve performance in high doppler rayleigh environments, that are representative of assets moving at high speed in urban environments, such as a helicopter in urban operations.

4.2.2 Background

Within this section the reader is provided a background on the NATO NBWF and some features that are important to be understood prior to the novel techniques and performance enhancements presented in this section.

4.2.2.1 Waveform Specification

The NATO NBWF was released by the NATO Line of Sight Capability Team (LOSCaT) as STANAG 5360 Edition 1 in April 2019, including the associated standards 5630-5633[104].

The NATO NBWF supports a number of different modes with various data rates, modulation parameters and coding rates. Modes N1 to N4 and NR provide burst data rates of 10 to 82kbps in a channel bandwidth of 25kHz. Modes N5 and N6 increase the signal bandwidth to 50kHz providing data rates of 40 and 63kbps respectively.

The testing described in this section focuses on the N1 mode specifically, as this is the fundamental mode of NBWF, although there is no reason why the techniques could not be applied to the other NBWF modes.

Prior publications on NBWF implementations have focused on low-complexity implementations [111] [232], however the novelty contained within this thesis is on a high-performance equalization approach and the performance of this in a simulated urban environment.

4.2.2.2 Continuous Phase Modulation

Abrupt phase changes in non-continuous phase modulation schemes such as QPSK result in high spectral side lobes and therefore poor adjacent channel leakage. In CPM schemes phase transitions are continuous and as such side lobes are kept to a minimum

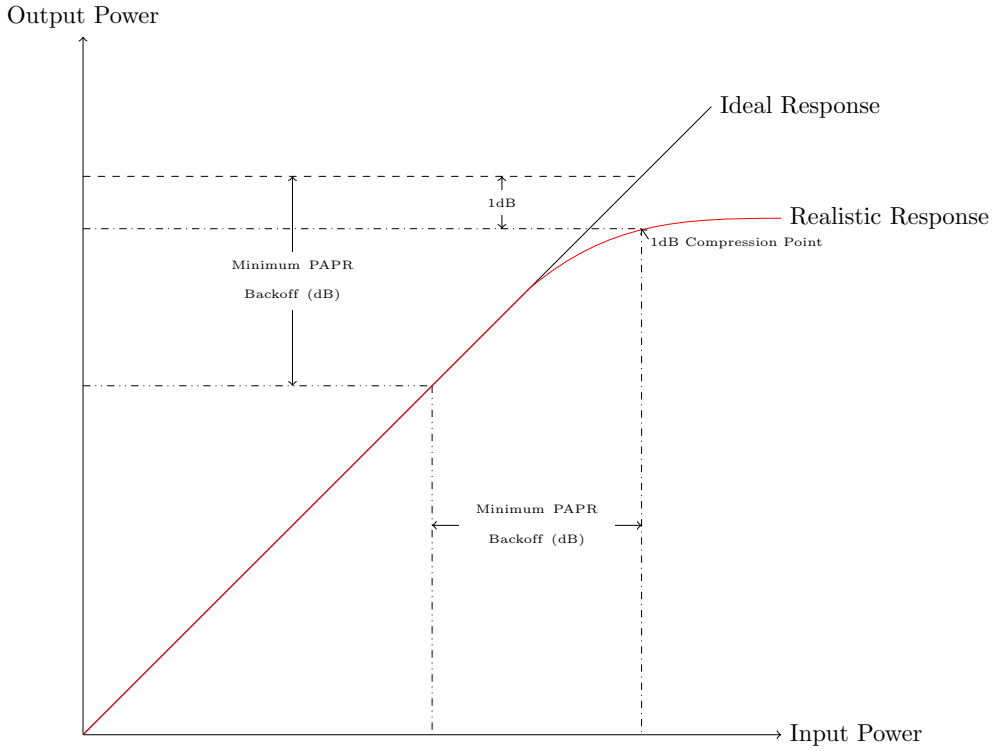


FIGURE 4.2.1: Ideal and Realistic Amplifier Responses demostrating impact of PAPR

which enable reduced adjacent channel leakage and high spectrum channelisation and utilisation.

A further benefit of CPM is that it has a constant envelope. Radios with size weight and power (SWAP) limitations must operate their amplifier close to saturation point in order to work at peak efficiency or to increase coverage in a tactical network. Modulation schemes with high peak-to-average-power ratios (Peak to Average Power Ratio (PAPR)), such as quadrature amplitude modulation (QAM) or CP-OFDM, cannot operate in this area as symbols at the peak power will be distorted by amplifier non-linearities. Whereas a constant envelope signal, such as that provided by CPM (or indeed Minimum Shift Keying, a variant of CPM) can operate close to this saturation point with limited signal degradation [233].

The impact of Peak-to-Average Power Ratio (PAPR) on the maximum power output can be observed in figure 4.2.1. This figure presents two curves: one depicting the ideal response and the other reflecting a realistic response. Noticeably, the amplifier saturates at a certain point for a given input power. When the output power deviates by 1dB from the ideal response, it is considered the 1dB compression point.

In practical deployments aiming to minimise distortions in the transmit chain, the transmitter must reduce the input power to keep the amplifier in the linear region. This practice, known as backoff, is crucial. The backoff value should match the PAPR of the input signal. Failure to do so could result in samples of the transmit chain

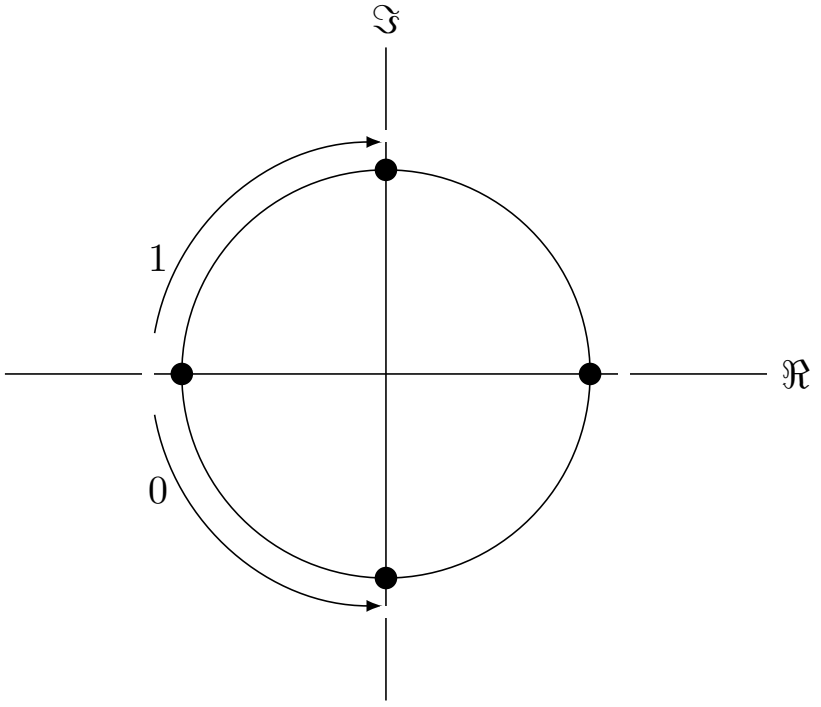


FIGURE 4.2.2: Constellation diagram representing CPM Schemes

surpassing the 1dB compression point, leading to signal distortion. For CP-OFDM, a recommended backoff is at least 12dB [234]. In contrast, CPM exhibits little to no PAPR, making even a 1dB backoff acceptable. This quality makes CPM a recommended waveform for tactical radio use cases, where output power is a key design consideration for systems.

This approach to modulation can be visualised in figure 4.2.2 whereby it is possible to observe how the information is encoded on the phase change between symbol periods, as such the transmitter remains at a constant power envelope. Furthermore, the diagram demonstrates that phase of the modulation must constantly be changing to transmit information and the importance of maintaining phase continuity with such CPM modulation schemes. This phase continuity is the prime motivator for the sub-block turbo equalizer as discussed later in this section.

CPM data rates can be increased, as with most modulation schemes, by reducing the symbol duration. This leads to an increase in spectral bandwidth of the waveform, which can be compensated for by reducing the size of the phase transition. Results displayed in this section use a ½ modulation index CPM, corresponding to maximum phase transitions of 90°, with a rectangular frequency pulse; this corresponds to the N1 mode in [104].

4.2.2.3 Turbo Equalization

Equalization is required in high multipath channels caused by mountainous terrain at the Very High Frequency (VHF) band or urban environments at the Ultra High Frequency (UHF) band. Traditionally equalizers have operated separately to forward error correction (FEC) decoders [232], with the equalizer passing information to FEC in the receive chain. This information may take the form of hard or soft bits, where soft bits encode both the expected value of the bit and the certainty of this value.

Given the performance of modern iterative FEC it is clear that this information need not pass in one direction. Turbo equalizers pass soft bits to FEC decoders which then produce their own soft bits to be passed back to the [235; 124]. This creates an iterative feedback loop improving Bit Error Rate (BER) performance at the cost of hardware complexity and latency. Typically turbo equalization relies on the Soft Input Soft Output (SISO) algorithms based on the forward backward algorithm of Bahl, Cocke, Jelinek, and Raviv (BCJR) [205].

Turbo equalization can be combined with any FEC that outputs soft bits in the form of logarithmic likelihood ratios (LLRs), however hardware complexity and SWAP considerations typically limit these to non-iterative decoders for tactical communications product offerings, in this case a convolutional code as shown in figure 4.2.5.

Equally turbo equalization can be combined with any single carrier modulation demapping approach, including QPSK, QAM and CPM as long as these output soft bits in the form of LLRs [236].

4.2.2.4 Convolutional Codes

Convolutional codes are a form of error correction originally introduce by Elias [123], with Viterbi proposing the first practical method of their maximum-likelihood decoding [237]. Check bits are created by convolving data bits according to a generator polynomial. Convolutional codes can be applied to blocks of any length, and when implemented in an iterative form, i.e. turbo codes [124] can benefit from belief propagation to achieve near capacity communications. Through the removal of a portion of the parity bits in a process known as puncturing, convolutional codes can provide flexible code rates without significant modification to the encoder or decoder.

The shift register used in LTE communications [238] can be seen in figure 4.2.3. In the LTE Convolutional coding process, a shift register is integral to the encoding mechanism. The shift register serves as a digital circuit that accepts incoming binary information at each clock cycle. Following this, a shift operation is performed, causing the existing bits within the register to move to the subsequent stage. Crucially, the

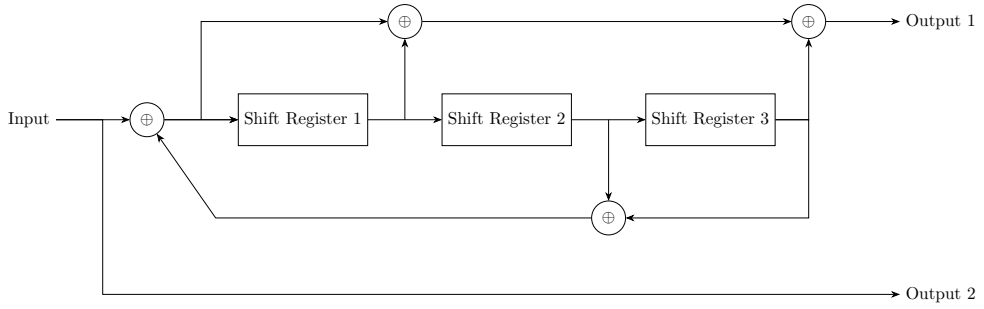


FIGURE 4.2.3: Shift Register for the Convolutional code used in LTE

shift register is intricately linked to a set of feedback connections that dictate how the bits are combined and reintroduced into the system. This interplay of shifting and feedback, determined by the convolutional code's generator polynomials, contributes to the generation of the convolutional code. The resulting output from the shift register forms the encoded bits used for error correction in LTE, aligning with the standards set for Long-Term Evolution in wireless communication [148].

Results displayed in this section use a ⅔ rate convolutional code, generated through a ⅓ mother code and a puncturing matrix defined for mode N1 of NATO NBWF [104].

4.2.3 Modelling Approach

4.2.3.1 Multipath Environment Channel Models

To assess the performance of the equalizers a frequency flat Rayleigh channel was modelled with varying SNRs. The Rayleigh channel was chosen as it represents the most extreme case of fading in the urban environment. The symbol duration of the NBWF N1 mode (33μs) is large relative to the delay spread expected in a dense urban environment (root mean square of order 1μs [239]), which suggests the individual signal paths are not resolvable to the receiver and therefore a frequency-flat distribution best describes the channel [240].

Channels were simulated with maximum Doppler shifts of 1.3, 3.9 and 9.1Hz corresponding to a 88MHz signal being received while travelling at 10, 30 and 70 miles-per-hour respectively. These Doppler shifts would correspond to significantly lower velocities at UHF frequencies. Channels were modeled using additive white Gaussian noise (AWGN) and a rayleigh fading channel.

Rayleigh channels were modeled with one and two resolvable paths. The second path has a delay of 20 microseconds and a relative signal strength of -5 dB, this corresponding to a helicopter travelling through an urban environment.

4.2.3.2 Channel Capacity

The channel capacity for a CCMC in an AWGN environment is defined by Shannon in [241] as shown Eq. (2.5).

Using (Eq. (2.5)) and with the knowledge that the spectral efficiency of NBWF mode N1, 0.8 bits/s/Hz, it is possible to calculate the CCMC capacity of an AWGN channel at the spectral efficiency of the N1 mode of NBWF as -1.3dB.

This CCMC capacity can be further utilised to understand how near capacity the BER performance of NBWF mode N1 is during the following sections.

4.2.3.3 Sub-Block Turbo Equalization

Fast fading and phase-inversion caused by strong multipath environments can result in poor equalizer and demapping performance, as the channel estimation provided by the synchronization sequence is only valid for a period of time shorter than the block length. This in turn causes poor BER performance for the entire receiver. Neito et al's turbo equalizer [242] was reproduced (hereafter referred to as the Full Block Turbo Equalizer (FB-TE)) and found to break down in some of these environments, even with an increased number of iterations.

To counter this a modification to the FB-TE was proposed: the Sub Block Turbo Equalizer (SB-TE). Incoming blocks are split into sub-blocks with overlapping symbols, as illustrated in figure 4.2.4. As a rule, the overlap length must be at least the sum of the modulator pulse length and the reciprocal of the modulation index. For N1 with a pulse length of two and a modulation index of 0.5 the minimum overlap length is 4; in this section the overlap length is set to five symbol durations.

These sub-blocks are equalized separately, with all but the first sub-block making no assumption on the initial phase. Instead the sub-block is equalized at a four different initial phases, with the optimum initial phase being judged as having the greatest sum of magnitudes of the output LLRs. The idea being that the equalizer can then limit impairments to a single sub-block, improving performance in fast fading channels.

Regarding complexity for the initial phase search space four phase variations are searched only in the initial three iterations, which quadruples the complexity in comparison to the FB-TE. Beyond these initial three iterations the complexity is similar to the FB-TE, with a small increase in complexity due to equalizing the overlapping sub-block symbols twice per iteration.

For both the FB-TE and the SB-TE the number of iterations per block was limited to 8. Increasing iterations leads to an increase implementation complexity and the number of operations required per block in a linear manner. Initial testing showed that

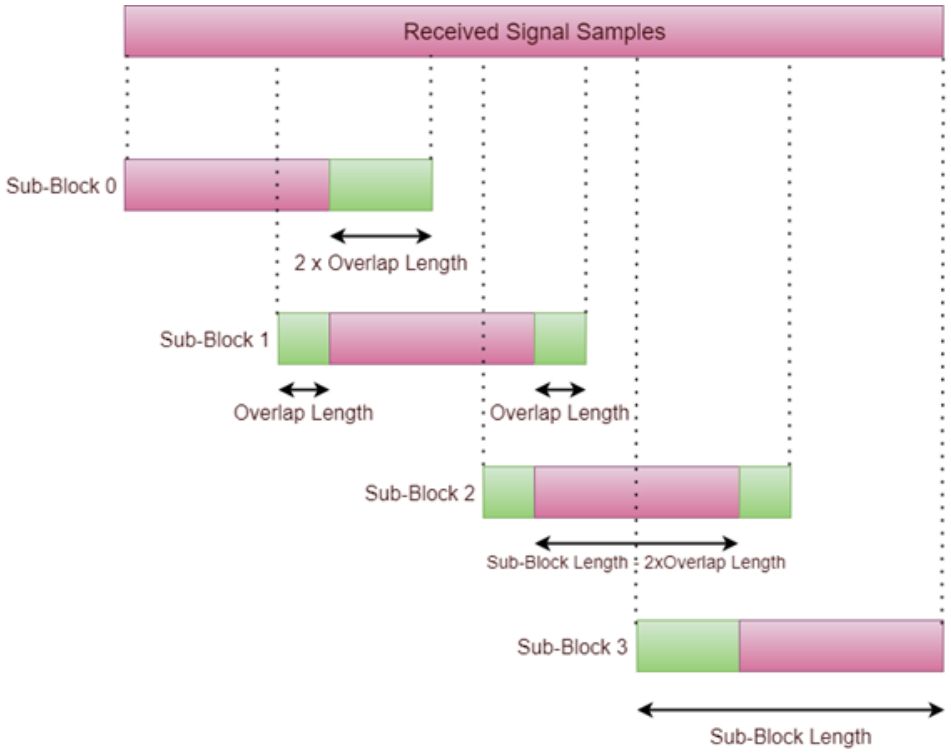


FIGURE 4.2.4: Method of splitting a received block into sub-blocks

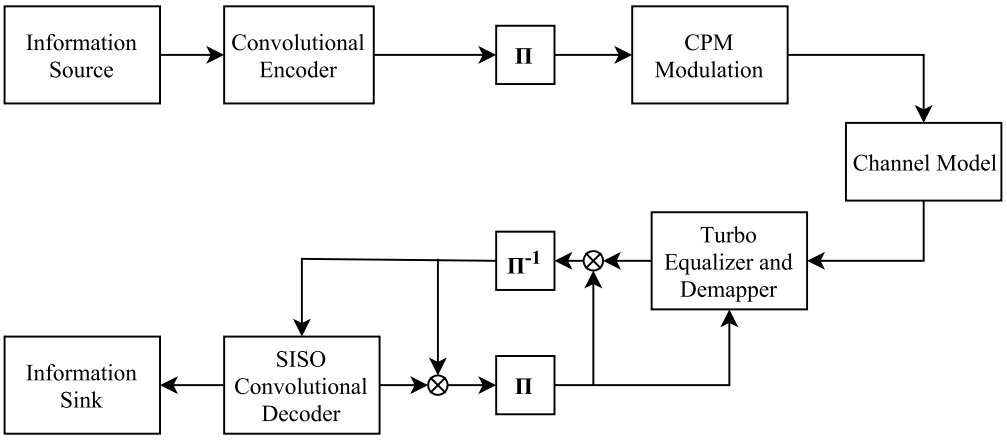


FIGURE 4.2.5: System diagram for a Full-Block Turbo equalizer

the improvement in BER going from 1 iteration to 8 was over an order of magnitude greater than going from 8 to 15, for the same increase in complexity.

The block diagram for the SB-TE is shown in figure 4.2.6, contrast this to the standard FB-TE shown in figure 4.2.5. Sub-block turbo equalization does not require alterations to the transmit sequence, therefore a receiver equipped with a SB-TE mode would be compatible with a transmitter that is not equipped with such a mode.

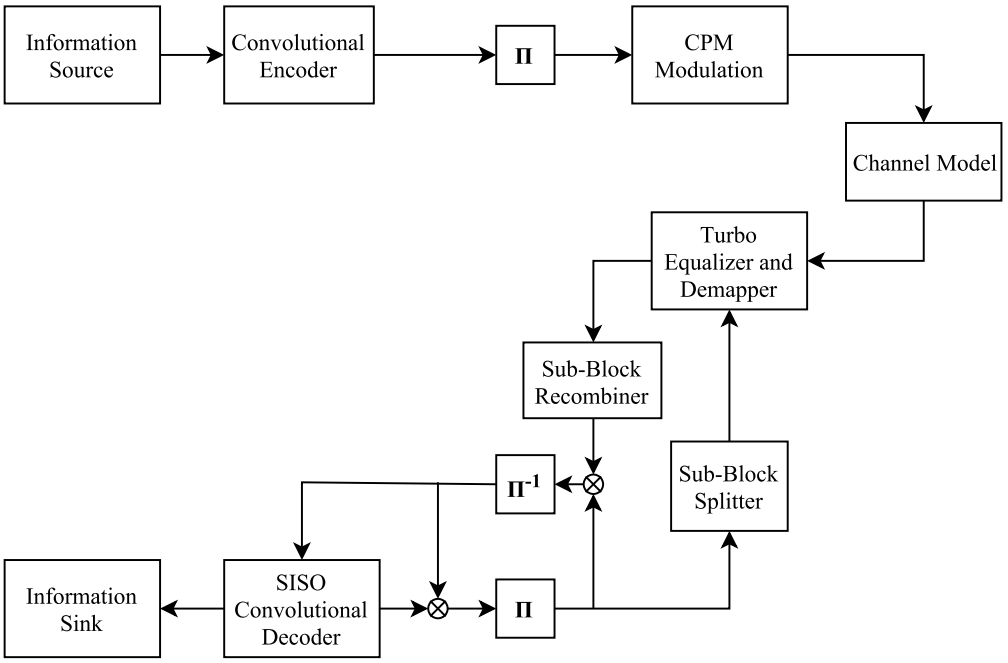


FIGURE 4.2.6: System diagram for a Sub-Block Turbo equalizer

4.2.3.4 EXIT Chart Analysis

EXIT charts are a common method of analysing iterative decoders first introduced by ten Brink in [103]. They represent the passing of information between components of the decoder, in this case between the equalizer and the convolutional decoder.

EXIT chart analysis allows for a deeper understanding of mutual information (I) transfer between two iterative code components, such as is observed with the Sub-block Turbo Equalizer, between the Turbo Equalizer itself and the SISO Convolutional Decoder.

When measuring mutual information, this can either be done using one of two methods, the first which is commonly referred to as the 'histogram method' uses the known a-prior bit values (0 or 1), their corresponding received LLRs and associated histograms, for which this method is detailed in [174]. The second, commonly referred to as the 'averaging method' where the average mutual information is measured for all LLR values across a frame. If the LLR generation and demapping function is built correctly, and the LLRs follow a Gaussian distribution, then both of these methods will provide the exact same output [243]. For this work the averaging method is use, which is described below and in further detail in [126].

For the averaging case, to calculate the mutual information (MI) it is possible to use Eq. (4.3) below, which is derived from Eq. (2.9) and Eq. (2.7).

$$MI = 1 - (-P_0 \log_2 P_0 - P_1 \log_2 P_1) \tag{4.3}$$

where P_0 and P_1 represent the probabilities of the specific LLR being decoded as a 0 or a 1 respectively.

On each of the composite components of an EXIT chart is the mutual information of the input of one component and the output of the other. For the sake of visual clarity axis labels are abbreviated; I is the of mutual information, the superscripts Eq and Dec denote whether the label is referring to the equalizer or the decoder and the subscripts i and o denote whether the information is passing in or out of the component.

Trajectories can be plotted between the curves to map the progress of decoding in a single block. If the trajectory is blocked by the overlapping of curves, for example in a noisy channel with insufficient error correction, then successful decoding is impossible.

Furthermore, it has been shown in [173] that the area between the EXIT curves (assuming that the inner code has a rate of 1) is shown to be the distance to channel capacity. In the case of the NBWF this is indeed the case, as the inner code can be seen to be the equalizer function itself, which has an inherent rate of 1. A further description on EXIT functions can be found in [174].

Predicted EXIT chart curves are created by generating LLRs with mutual information values between 0 and 1 and passing these through each component to generate the output information point. As the equalizer is also dependent on the SNR of a received signal, random bits are modulated then passed through a AWGN channel and fed into the equalizer with the input LLRs.

4.2.4 Results

In this section the FB-TE and SB-TE are compared using the NATO NBWF mode N1, performance is analysed in Rayleigh fading channels with maximum Doppler shifts of 1.3, 3.9 and 9.1Hz corresponding to a 88MHz signal being received while travelling at 10, 30 and 70 miles-per-hour respectively

4.2.4.1 EXIT Trajectories

As shown in figure 4.2.7 the EXIT tunnel and therefore associated decoding path opens for the FB-TE at an approximately SNR of -0.2dB implying it is 1.1dB from channel capacity in AWGN conditions. It should be noted that a practical system would fail to decode at these SNRs as it would require an unworkably high number of iterations to achieve successful decoding, however this enables a strong prediction of when the turbo equalizer will start to converge. This EXIT tunnel opening at -0.2dB maps well with the convergence of both the FB-TE and SB-TE in figure 4.2.9.

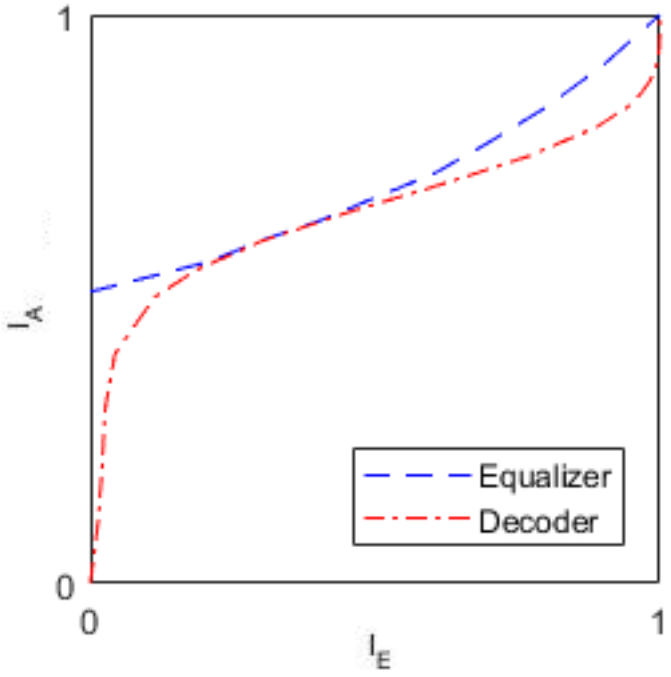


FIGURE 4.2.7: EXIT chart for the FB-TE with a ⅔ rate convolutional code opening at an SNR of -0.2dB

For illustration, figure 4.2.8 shows an example EXIT tunnel now open at a SNR of 1dB. In this case, the block is fully decoded after three iterations.

4.2.4.2 Bit Error Rates

The BER performance of the full- and sub-block turbo equalizers are compared in various channels. Performance in Rayleigh channels was analysed with maximum Doppler shifts of 1.3, 3.9 and 9.1Hz corresponding to a 88MHz signal being received while travelling at 10, 30 and 70 miles-per-hour respectively. To reflect the performance of the modulation scheme and turbo equalizer alone, transmit and receive filters were not used and perfect initial synchronization was assumed in the generation of these results.

Figure 4.2.9 demonstrates that the FB-TE outperforms the SB-TEs in an AWGN channel. This is to be expected as the splitting of the sub-blocks limits equalization travelling across the divisions. However, as shown in figure 4.2.10, in a Rayleigh channel with a maximum Doppler shift of 9.1Hz the FB-TE fails to achieve an acceptable BER while the SB-TE continues to show improvement at increased SNRs.

It is interesting to note that at SNRs above 15dB, the results indicate that the SB-TE becomes more resilient to errors with increasing Doppler shifts. It is believed that this

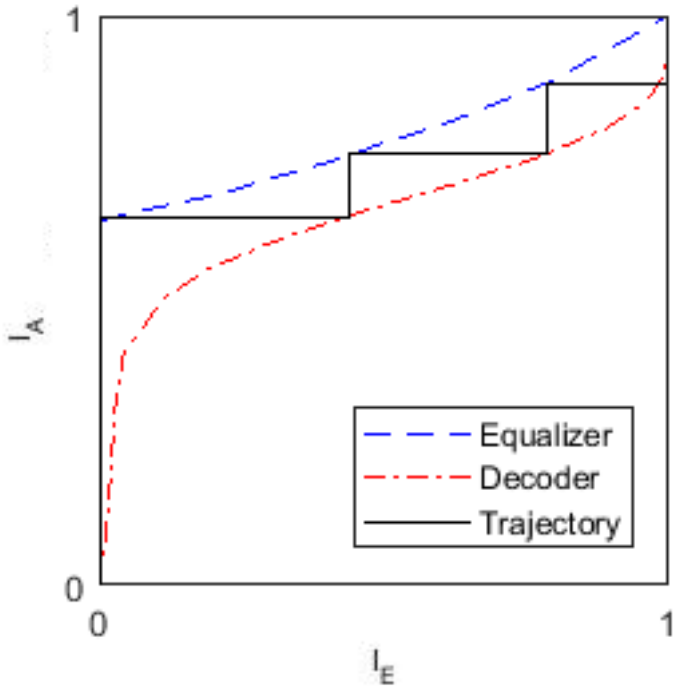


FIGURE 4.2.8: EXIT chart for the FB-TE with a ⅔ rate convolutional code open at an SNR of 1dB.

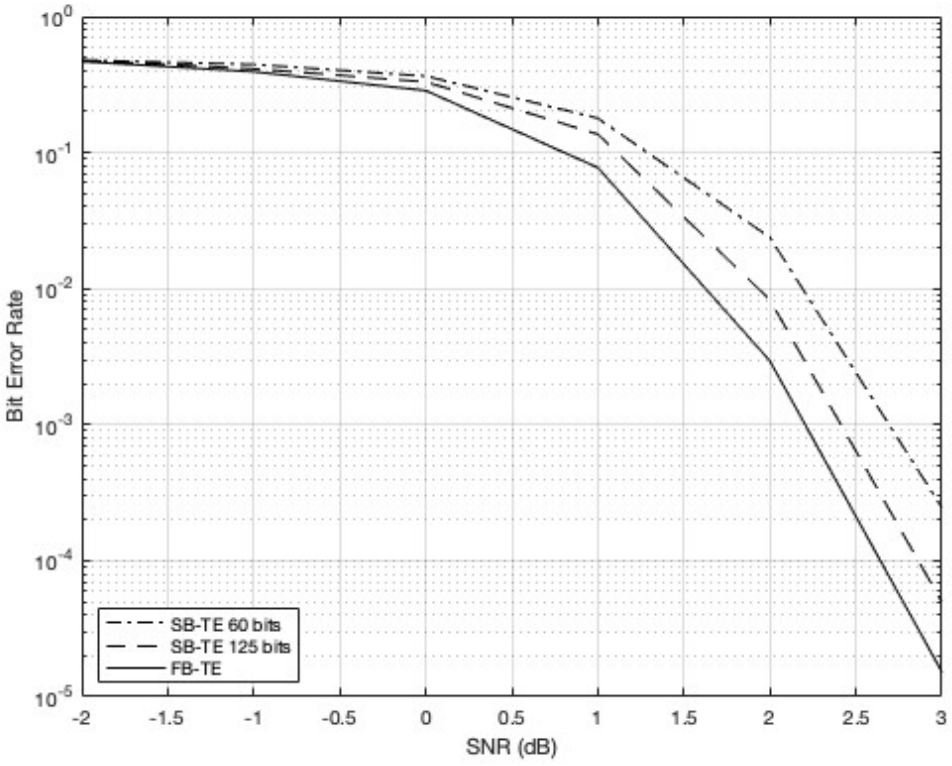


FIGURE 4.2.9: BER curves for the FB-TE and SB-TEs turbo equalizers in an AWGN channel

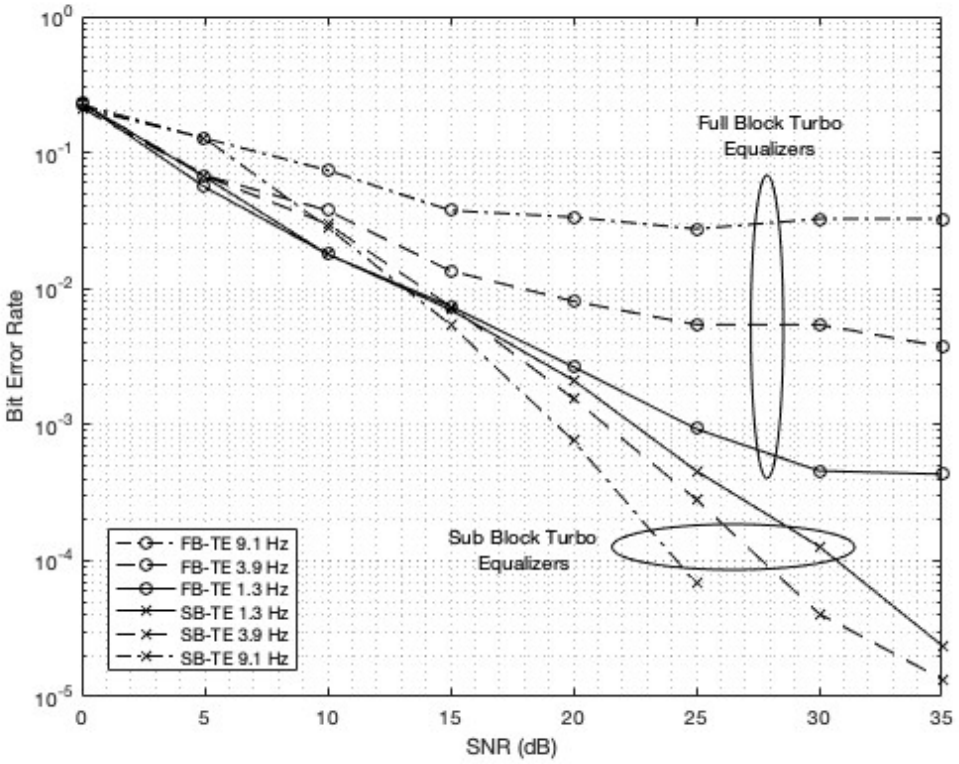


FIGURE 4.2.10: BER curves for the FB-TE and SB-TE with 125bit sub-block length in various Rayleigh channels

is due to the overall frame-length becoming long enough relative to the fade period, such that time diversity can be extracted from the channel. It is likely that this effect is not observed in the FB-TE due to error extension caused by rapid phase changes not enabling the equalizer and CC to converge over the full block. A possible area of future research is to analyse the dominant error mechanism at these high SNRs, in order to further optimise the SB-TE and clarify that these are reasons for these observations.

4.2.4.3 Complexity

As noted in Section 4.2.3.3, SB-TE leads to an increased complexity compared to FB-TE. Table 4.2.1 quantifies the relative complexity of the equalizer functions by assessing the increase in repetition of symbol level equalizations when moving to the SB-TE. There is no increase in complexity from the convolutional code decoder associated with moving from the FB-TE to the SB-TE. The relative mean processing time for MATLAB implementations of the turbo equalizers (excluding the error correction) is also recorded, averaged over two thousand blocks and run on a Intel i5-8250u processor. As MATLAB is a high level scripting language, these figures may not be representative of hardware implementations. For example, as each sub-block can be equalized separately, the SB-TE would lend itself well to parallel processing.

TABLE 4.2.1: Relative complexity of turbo equalizers at eight iterations

	Relative complexity	Relative processing time
FB-TE	1	1
SB-TE 125 bits	1.9	2.7
SB-TE 60 bits	2.1	3.1

As shown in Table 4.2.1, both the complexity and processing time assessments agree that equalizing the smaller 60bit sub-block size is approximately 15% slower than the 125bit sub-block size. In both assessments the FB-TE is the faster equalizer, however there is a small disagreement as to exactly how much faster.

4.2.5 Discussion

The results found during the course of the research on NATO NBWF demonstrate that in order to use single carrier CPM waveforms, as is used for NATO NBWF, in fading channels (such as those found in urban environments where deep fades are expected across the time period of a frame) a SB-TE approach is likely to provide enhanced performance over FB-TE. These channels are more common at the higher frequencies which the NATO NBWF might be used. These performance improvements come at the cost of increased processing time and slightly degraded performance in AWGN channels.

Previous work has shown that similar waveforms begin to exhibit an error floor when the delay spread reaches 33% of the symbol duration [112], which could correspond to the N4 mode received over mountainous or hilly terrain. Further work is required to assess the SB-TE in the channels described in [112] as well as those in Annex C of AComP 5631 [104].

An alternative method to improve performance in such channel conditions would be to include reference symbols within NBWF slots, rather than just at the beginning of each slot. This would allow the equalizer to receive an updated channel estimate without the additional processing on the receive side required by SB-TE.

Furthermore, within this section it has been shown that EXIT chart analysis of NBWF can be used as a predictor for the convergence of both the FB-TE and SB-TE; via EXIT analysis it can also be shown that the NBWF N1 mode has a near-capacity performance with an EXIT tunnel opening at 1.1dB from the CCMC capacity.

4.3 Chapter Conclusion

Chapter 4 has introduced groundbreaking techniques that improve the performance of tactical communications systems.

It has presented a novel approach for demodulation of M-ary Orthogonal Signalling which addresses a critical limitation of current methods [109], eliminating the reliance on hard-decision approaches and potentially enhancing performance by 2 or 3dB.

Furthermore, a novel equalisation approach, tailored for differentially encoded modulation schemes in challenging environments, has been presented. The evaluation of this scheme in Rayleigh fading channels has been undertaken, simulating tactical urban deployment scenarios which demonstrates significant improvements, especially in scenarios with rapid phase inversions, typical of deployment scenarios faced by helicopters where traditional equalizers may falter. The scheme has also undergone EXIT chart analysis, as was introduced in Chapter 2 of the thesis.

This chapter represents a substantial advancement in addressing practical challenges in wireless communication, particularly in complex and dynamic deployment environments.

The thesis will now delve into the depths of some specific deployment scenarios and specific channels within Chapter 5, whereby the realm of tactical communications in underwater environments will be explored, elements as introduced in Chapter 4 will be further explored with the use of M-ary orthogonal signalling within the Phorcys communications protocol stack.

Chapter 5 : Tactical Communications in Underwater Environments

This chapter can be seen within the structure of the overall thesis in figure 5.1.1. Within this chapter aspects of tactical communications in underwater environments are explored. The majority of the chapter focuses on secure underwater acoustic communications with an emphasis on standards and their impact on a variety of underwater operations.

This chapter delves into the various technological domains explored throughout the thesis with a specific view towards underwater environments. It encompasses a exploration of information sources pertinent to the underwater domain, including the encoding processes employed. Furthermore, this chapter analyses and proposes novel

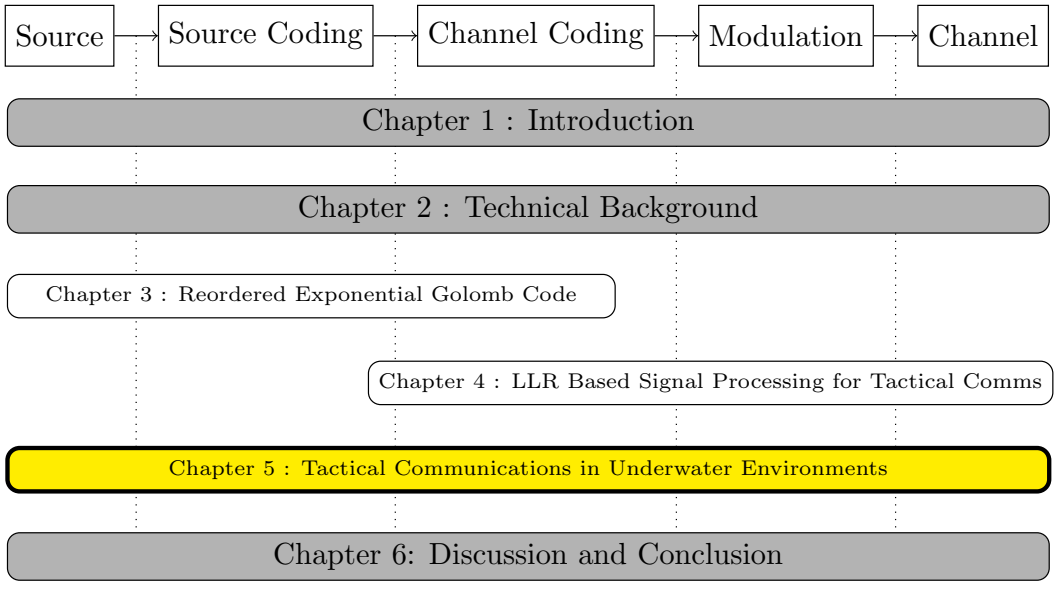


FIGURE 5.1.1: Structure of the Thesis

FIGURE 5.1.2: Structure of Chapter 5

approaches to modulating and encoding this information onto communication channels, thereby facilitating effective transmission in an underwater environment.

In this chapter, a multitude of techniques are proposed, foremost among them being the innovative Phorcys communications protocol suite. Developed and architected by the author of this thesis and validated through sea trials, networking evaluations, and performance criteria which were conducted in collaboration with others, the Phorcys communications protocol is uniquely designed to address interoperability needs for the underwater domain that existing standards do not cover. Subsequently, the chapter introduces novel approaches to integrating autonomy and underwater communications, expanding the operational capabilities available for underwater missions beyond current standards. Notably, segments of this chapter draw from various published research materials, including [1; 3; 2; 7; 6; 5; 244; 98]. The work presented in this chapter is the sole product of the author of this thesis, unless otherwise declared.

The overall structure of this chapter is presented in figure 5.1.2, which provides the reader with a high-level overview of the work discussed within this chapter. This chapter covers the breadth of the thesis with some emphasis on source coding, but the main emphasis being on channel coding, modulation, and channel aspects.

The chapter leads the reader through the variety of published works that present an overall narrative of work conducted and architected by the author in the field of underwater acoustic communications, previous attempts to deliver a communications system for underwater communications have either focused on individual aspects of a communication system [7; 113; 114; 115; 116; 117] or a minimum viable product for interoperability [118], with little emphasis on either performance or security. Within this chapter a new approach that is holistic in nature, and considers the security requirements of the nature of operations is introduced. This has led to the specification of the Phorcys protocol suite [109] which aims to be adopted by NATO to meet these operational needs, and the work which has been led and undertaken by the author is presented within this chapter.

The author of this thesis has led UK efforts through the Phorcys and Venilia projects, as well as being a leading national representative of the JANUS Support Team within NATO, and the chair of a NATO Research Task Group on secure underwater communications. The work presented in this chapter is that which can be presented as the work of the author to contribute to this thesis; however the author has been leading substantial teams to develop this into wireless communications standards, and operational capability.

Aspects of Chapter 5 have been published in a number of papers and represent a small section of the work the author has led on the Phorcys communications protocol stack development, which the author has led and architected while in tenure within the UK government. Aspects of these sections are published in [3; 7; 6], and the work in this chapter solely represents the author's contribution. Furthermore, other aspects of Chapter 5 represent the work the author has led on Venilia to develop a new secure class for JANUS; parts of this section have been published in [244] and [2]. There also contains contributions to Chapter 5 which relate to collaborative work on the integration of communications and autonomy published in [1]. The items from these papers presented within this thesis represent the sole work of the author of this thesis.

The novel work within this chapter is based upon realistic operational and environmental conditions, which are described in the following section. As these operational scenarios are explored, it clarifies that the extant standard for digital underwater communications, JANUS [245; 118], is not designed to meet the needs of brevity, security or networked performance that are required of these scenarios. Therefore, the schemes proposed within this chapter are designed to meet these operational requirements and achieved similar or greater range requirements whilst improving performance in nearly all other areas.

Within the next section, two of these scenarios which are able to be discussed openly within this thesis will be explored.

5.1 Underwater Communications Environment and Deployment Scenarios

Aspects of this section have been published in [1] and the use cases, which were derived from NATO use cases are deemded unclassified, and underwent the UK Government 'permission to publish' process to be deemed suitable for publication in [1].

Within this section we will explore the use cases that are enabled by underwater communications and some of the environmental and deployment aspects relating to underwater operations.

5.1.1 Use Cases

Many maritime warfare disciplines have witnessed an increasing interest in the use of autonomous assets to perform the so-called dull, dirty, and/or dangerous activities. Such autonomous assets provide significant capability potential because they can be deployed in large numbers and conduct cooperative tasks. However, cooperation is limited by the amount of data underwater communications can reliably provide. In the underwater environment, both radio and optical signals are greatly attenuated [246; 96], and acoustic waves remain the most efficient means to communicate underwater for ranges beyond about 50 m [247; 113]. Nonetheless, acoustic-based underwater communications suffer from long propagation delays and low data rates. Factors affecting the quality of the received signals include extended reverberation, frequency-dependent absorption, high motion-induced Doppler, and site-specific plus cyclical (i.e., tidal) ambient noise [248].

In addition to these challenges, the lack of secure underwater digital communications standards represents a major bottleneck for supporting NATO operations such as Rapid Environmental Assessment, Mine Countermeasures, Anti-Submarine Warfare, Underwater Maritime Situational Awareness, and Search and Rescue (SAR). It is essential to enhance the resilience and assurance of underwater communications through improved security awareness (e.g., confidentiality, authentication, integrity protection, jamming detection) and improved security measures (e.g., counter-interception by encryption, anti-jamming/spoofing/tampering/hacking).

Existing underwater acoustic communications technologies, such as the JANUS standard [245; 118] (which will be further explored in this chpater) do not consider security as a performance indicator and focus on software/hardware implementation, range coverage, and achievable data rates [249]. Limited studies on underwater network security have appeared in the open literature ([250] and references therein). Additionally, existing security solutions in terrestrial networks cannot be applied directly due to the stark differences between underwater acoustics and radio channels.

Hence, an attacker could easily compromise an underwater acoustic network in numerous ways, such as jamming [251; 252], leakage of confidential data [253], re-routing of transmitted information [254], message replay [255], just to name a few.

Specifically, two use cases are presented in this section: Mine Counter Measures and Anti-Submarine Warfare. A traditional Mine Counter Measures (MCM) operation involves a fleet of surface and subsurface platforms working in unison to identify and neutralise subsurface targets. This will most often be in completely unknown environments, with little opportunity for reconnaissance. Anti Submarine Warfare (ASW) operations can take place in both known and unknown environments. There may be historical bathymetry data available, but this is not guaranteed. This operation relies on a fleet of subsurface vehicles collecting data on possible targets and reporting this to a remote data sink. There may be additional requirements for covertness. Both of these operations are expected to be carried out in littoral waters, and any live data will need to be distributed across all users within the network.

5.1.1.1 Autonomous Mine Counter Measures MCM

In this scenario (figure 5.1.3), a fleet of autonomous underwater vehicles (AUVs) is deployed as a networked swarm into the operating environment. The mission is controlled from a surface vessel, which maintains contact with the underwater fleet via acoustic communications. The AUV network must gather data on the targets; this data may consist of side-scan sonar data, images from on-board cameras, and the location of the target from on-board position estimates. The data can either be processed locally or transmitted to the surface vessel for further analysis.

The geographical environments for which mine countermeasures are likely to be utilised will be shallow water environments, where an acoustic line of sight may not exist. Furthermore, to reserve battery power on AUVs, they will most likely wish to remain submerged and on task, being provided with command and control and navigation information sub-surface. All nodes should be aware of the capabilities possessed within a mixed fleet autonomous mine countermeasures environment and how each can be tasked to most efficiently achieve the overall mission aim.

Local processing would involve running some target recognition algorithms over the data, which would significantly reduce the amount of data needed for transmission back to the base station. However, this incurs significant processing overhead and may be infeasible on low-powered platforms, and the operators must accept the risks posed by inaccurate target recognition algorithms. Transmitting all of the data back to the surface vessel places a significant burden on the low data rate acoustic communications links available.

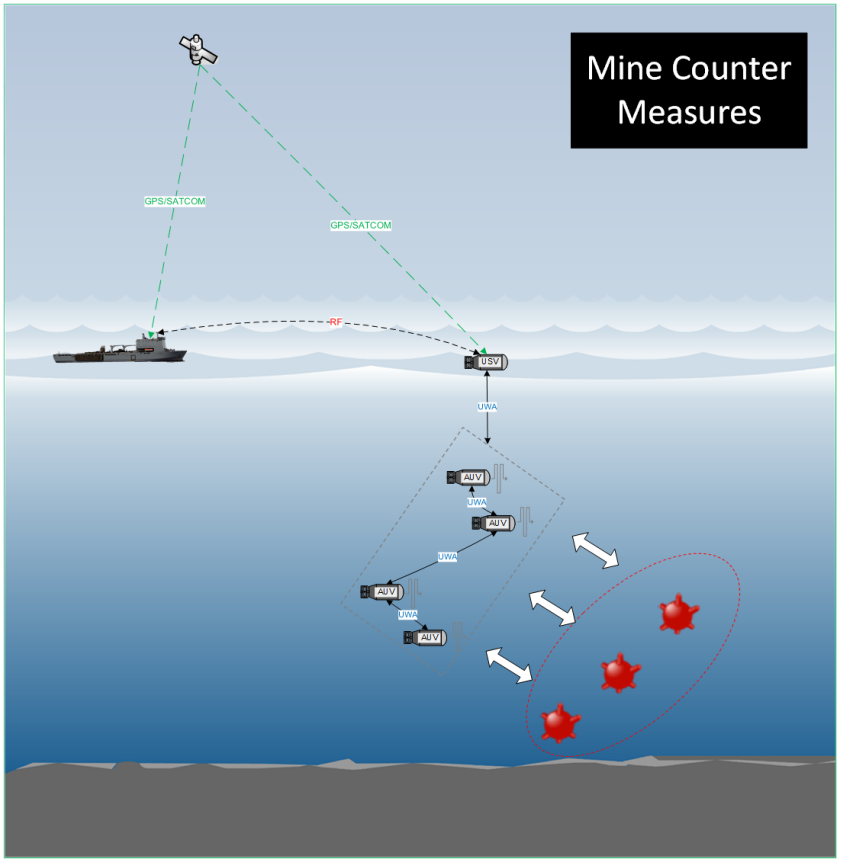


FIGURE 5.1.3: Mine Counter Measures Use Case. The AUVs communicate over acoustic channels, reporting collected data back to the command station through an Unmanned Surface Vehicle (USV). This surface vehicle is localised via GPS.

It is envisaged that for future autonomous mine countermeasures operations, a mixed fleet of AUVs will be used with more than 10 platforms, for accurate and rapid assessment of the environment.

5.1.1.2 Anti-Submarine Warfare (ASW)

The ASW scenario (figure 5.1.4) comprises a network of AUVs stationed in a geo-stationary defined area, trying to detect any submarine platforms that are present. This detection could be achieved through passive arrays, as part of a multi-static active network, or other variations. This data must then be returned to an operational commander to provide situational awareness. An ASW operation could persist over a long time period and might not have a defined end date. The AUV nodes will likely be collecting sonar data or passive hydrophone recordings. Once again, this data can either be processed locally or transmitted to the command node for processing.

Unlike the mine countermeasures scenario, actual detection events are likely to be very rare. Instead, most traffic will likely be network management (vehicle status, location reporting, etc.) or false positives. The network will either need to provide a data rate

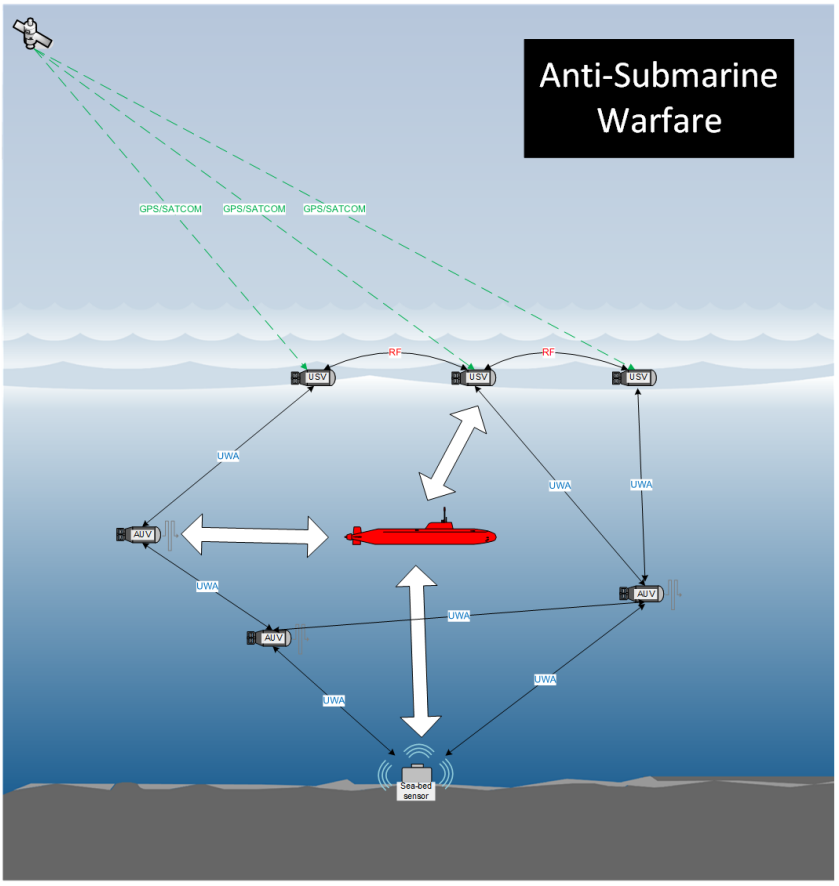


FIGURE 5.1.4: Anti-Submarine Warfare Use Case. A network of USVs identifies a hostile platform and informs a remote command post via a satellite link.

high enough to support the transmission of these false positives or filter them out. Additionally, there may be a requirement for the AUV network to operate with a reduced acoustic signature to reduce the likelihood of an adversary detecting the presence of the ASW operation.

As with MCM, an ASW scenario utilising autonomous systems will probably comprise a large mixed fleet in excess of 10 platforms. Furthermore, ASW operations are likely to occur in slightly deeper water whereby shadow zones caused by acoustic sound channels will come into effect, both disrupting communications, but also being able to hide potential contacts.

Following on from these deployment scenarios, there are a number of environmental concerns that must be considered when utilising underwater communications, specifically acoustic communications.

Unlike radio communications, the underwater acoustic spectrum is unlicensed and as such does not have any power constraints to reduce co-channel or adjacent channel interference. Therefore, there is a strong drive for energy-efficient communications schemes, as will be discussed in the following subsection.

5.1.2 Environmental Impact of Underwater Communications

Reducing the energy consumption of underwater communications is imperative for achieving efficient transmissions, thereby mitigating the environmental impact associated with increased energy efficiency.

This section elaborates on two key motivating reasons for enhancing the energy efficiency of underwater communications.

5.1.2.1 Battery Usage

The proliferation of Autonomous Underwater Vehicle (AUV) in underwater operations is increasingly prevalent [256]; refer to Section 5.5 for detailed insights into these specific operations. The heightened deployment of autonomous systems and battery-powered leave-behind systems, such as those utilised by the oil and gas industry for acoustic release systems, underscores the importance of minimising the energy expended in each transmission for any underwater communications protocol. Reduced power load during communications empowers devices to conserve energy, facilitating prolonged periods in a sleep state, supporting more power-intensive operations, or contributing to an extended mission duration.

5.1.2.2 Reduced Harm to Cetaceans

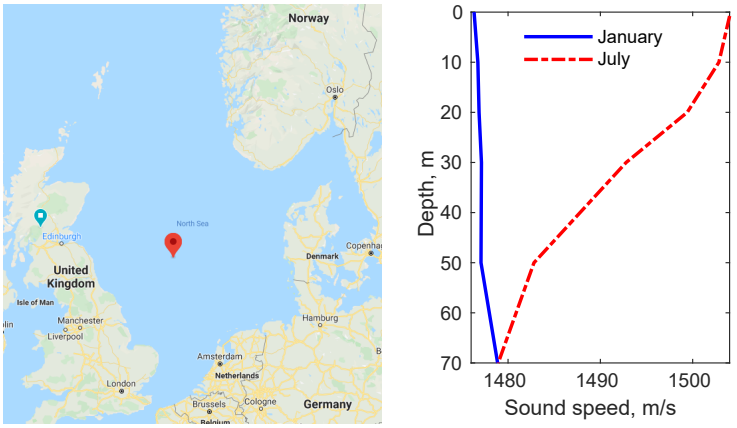
Acoustic communications, utilising pressure waves akin to SONAR, can adversely affect marine mammals and cetaceans [114]. This impact manifests through either damage to natural tissues [257] or the generation of excessive noise interfering with natural cetacean communications, thereby impeding the interactions of ocean wildlife [258].

Therefore, it is imperative to ensure that any acoustic transmission adheres to stipulated safety levels and maintains a minimum source power level, mitigating potential harm to natural wildlife and cetaceans.

For a coherent source (such as that which may be part of an underwater communications protocol), it is recommended withi the NATO Sonar Acoustics Handbook [246] that a source power level of 170 dB dB re 1 μPa @ 1m shall not be exceeded within 24 hours for MF cetaceans.

5.2 Underwater Acoustic Communications Propagation

To support the operational scenarios discussed in the previous section, effective communication over long and medium distances through water is imperative. Several



(A) Google Maps location

(B) Sound speed profile

FIGURE 5.2.1: Sound speed profile examples in January and July, based on the temperature, pressure and salinity data in the North Sea at (55.5^{o}N, 2.5^{o}E). From co-authors in [1].

communication mediums, including acoustics, optics, and electromagnetic methods, can be considered as have been in [2]. However, for reliable communication at distances exceeding 100 meters, acoustics stands out as the only dependable medium [116].

Acoustic communications exhibit variable speeds influenced by diverse environmental parameters, as elaborated below. It is essential to note a significant disparity between acoustic communications and other mediums, primarily in the speed of propagation, typically around 1500 m/s [259].

5.2.1 Acoustic Channels

In addition to its inherently slow nature, the propagation speed of acoustic waves varies in space and time, depending on factors such as water temperature, pressure, and salinity [260]. In figure 5.2.1 we illustrate two sound speed profiles derived by Dushaw [261] from the 2009 World Ocean Atlas data for January and July in the North Sea at (55.5^{o}N, 2.5^{o}E). In this relatively shallow water example, water temperature significantly influences sound speed, leading to notable variations in the sound speed profile between January and July. Warmer water near the sea surface in July results in a distinct negative sound speed gradient caused by the thermocline. These variations in sound speed at different depths induce refraction of acoustic waves towards the lower sound speed region, resulting in curved propagation trajectories forming waveguides, known as deep sound channels around a particular depth (where the sound speed is at its minimum). For instance, the sound speed profile shown in figure 5.2.1b cause downwards refraction towards the seabed in July but slight upwards refraction in January, significantly impacting network connectivity and link quality.

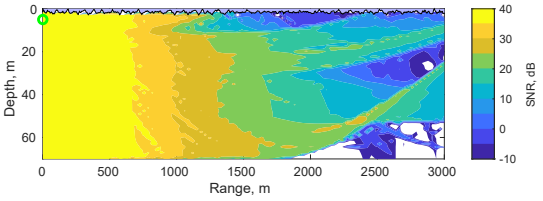
Figure 5.2.2 illustrates the spatial variability in the quality of the underwater acoustic channel, contingent upon the sound speed profile and the source's location within the water column. The contour plots depict the SNR calculated using the channel modelling framework detailed in [262], employing BELLHOP beam tracing [263]. This simulation incorporates randomly generated surface waves and utilises the January and July sound speed profiles from figure 5.2.1b.

The BELLHOP outputs were further processed with a centre frequency of 24 kHz and a bandwidth of 7.2 kHz, representative of typical wideband underwater acoustic transmissions [264]. This processing involved integrating the absorption loss for each traced multipath component across the entire frequency spectrum, resulting in the wideband received signal power (as detailed in [262]).

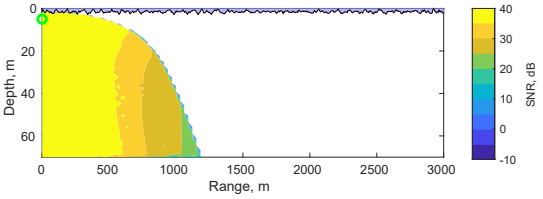
SNR values were then computed by dividing the wideband received signal power by the noise power, calculated using the ambient underwater acoustic noise model outlined in [247]. Assumptions for this calculation included a wind speed of 10 m/s, a shipping activity factor of 0.5, and a centre frequency of 24 kHz with a bandwidth of 7.2 kHz, corresponding traces are shown in figure 5.2.2 with a source power of 180 dB re 1 μPa @ 1m.

The plots in figure 5.2.2 illustrate the impact of the negative sound speed gradient in July, where downward refraction constrains the communication range to approximately 1-1.8 km, contingent on the depths of the source and receiver. Notably, these simulations adopt the generic BELLHOP seabed setting, featuring a flat surface modelled as an acousto-elastic half-space with a sound speed of 1600 m/s and a density of 1 g/cm^3 (representative of sand-silt [265]). Different bathymetry could potentially yield usable underwater acoustic communication links through seabed reflections. In contrast to the July results, figures 5.2.2a, 5.2.2c and 5.2.2e demonstrate that the absence of a thermocline in the January sound speed profile leads to more horizontally propagated acoustic waves, resulting in, most cases, an extended communication range (with the exception of seabed-to-seabed communication, where downward refraction in July is generally more favourable).

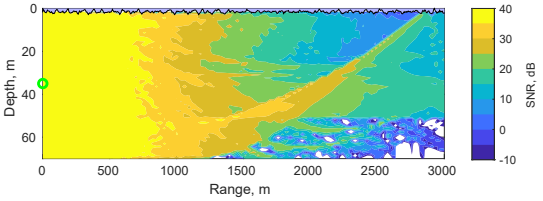
The different rows of plots in figure 5.2.2 reveal the influence of varying the source depth on the coverage area and channel quality of underwater acoustic communication. These plots showcase the formation of sound channels and acoustic shadows at different geographical locations, contingent on the sound speed profile and source depth. For instance, the slight upwards refraction in January gives rise to sound channels with high Signal-to-Noise Ratios (SNRs) at relatively long ranges (e.g. figures 5.2.2a and 5.2.2c), presenting opportunities for high-quality underwater acoustic communication when the source and receiver are strategically positioned in the water column. Conversely, optimal positioning of underwater nodes involves avoiding acoustic shadow zones and regions of low SNR to enhance the reliability of



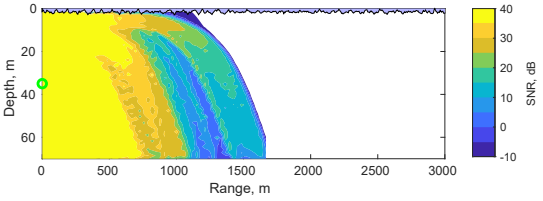
(A) January sound speed profile, source at 5 m depth



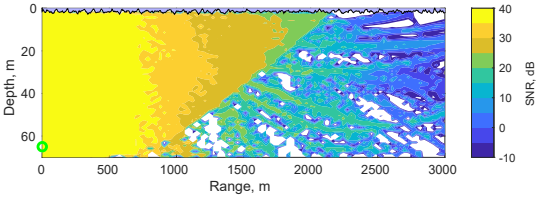
(B) July sound speed profile, source at 5 m depth



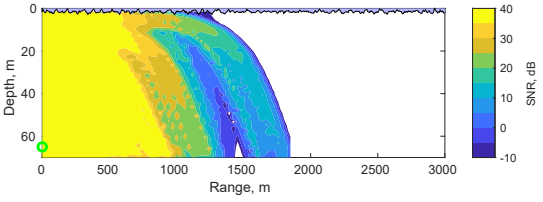
(C) January sound speed profile, source at 35 m depth



(D) July sound speed profile, source at 35 m depth



(E) January sound speed profile, source at 65 m depth



(F) July sound speed profile, source at 65 m depth

FIGURE 5.2.2: Signal to Noise Ratio (SNR) computed using beam tracing simulations of the North Sea environment

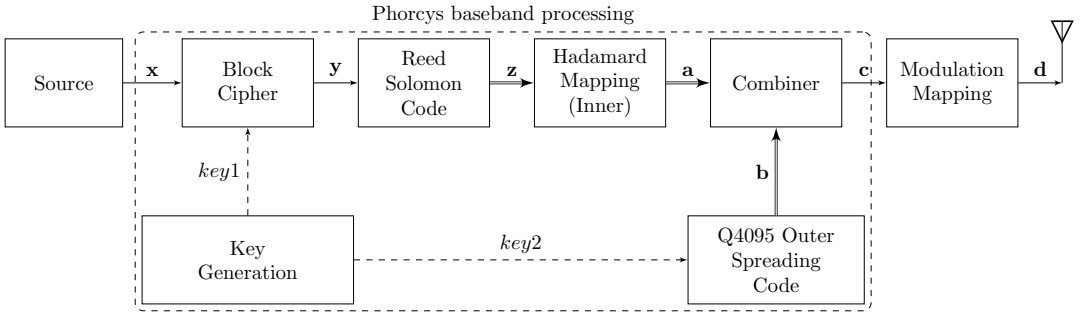


FIGURE 5.3.1: Phorcys Transmit Chain Block Diagram

communication links. A noteworthy feature of the autonomous subsea systems explored in this chapter, specifically in section 5.5, is their capability to adapt to the underwater acoustic propagation environment, enhancing the quality of communication among network nodes with minimal disruption to their primary missions, as discussed in Section 5.5.2.

5.3 Physical Layer Aspects

Enhancing the capability to conduct underwater operations safely, securely, and expeditiously is contingent upon the establishment of reliable, secure, and effective long-range communication, as extensively discussed in the preceding sections.

In this section and within this chapter, we propose the adoption of the Phorcys communications protocol suite as an evolutionary advancement beyond JANUS. Specifically, we advocate for Phorcys as a high-performance physical layer component within the conceptual framework termed the 'House of JANUS' [3] as will be introduced in section 5.6. This framework offers options for open, inherently secure, and highly resilient communication protocols designed for underwater communication scenarios.

Phorcys represents a pioneering protocol stack designed for adaptable and secure underwater acoustic communications. It utilises a shared "Gorgon" baseband processing foundation, featuring tunable parameters such as channel characteristics, bandwidth, Direct-Sequence Spread-Spectrum (DSSS), and M-ary Orthogonal Signalling (MOS). Consequently, Phorcys empowers users to customise their own trade-off between bitrate and resilience, tailored to the specific requirements of any underwater environment.

The generic block diagram for the Phorcys communications scheme is illustrated in figure 5.3.1, introducing the concepts of inner and outer spreading codes as discussed in this chapter, along with their relation to security and key generation. An input bit

stream is fed into the block cipher **x**, which undergoes block encryption—its overall size is variable. Following encryption, the bit stream is encoded into ciphertext **x**, which becomes Reed-Solomon symbols with coding rates of 0.68 or 0.52 and sizes of 63 or 42 bits, denoted as **y**. This vector is then split into 6-bit symbols, directly related to the M-ary orthogonal signalling discussed in Chapter 3. Subsequently, it undergoes Hadamard mapping, producing the bit vector **a**, which has a length of 64, as discussed in Chapter 3. Due to the same issues related to auto-correlation discussed in Chapter 3 regarding the Hadamard code, the bit stream is combined with the output of the Q4095 code, which is a high-performance auto-correlation code of 4095 bits in length, known as the complex vector **b**, in the combiner block.

Within this combiner block, each sequential 64-bit vector **a** undergoes an exclusive OR operation in the real domain with a sub-section of **b** until all information symbols sent in **x** are encoded. Once all information symbols are encoded, the output vector **c** is generated, which is then modulated based on the chosen modulation scheme (QPSK or BFSK) and the desired output frequency band, resulting in the output vector **d**. Throughout the encoding process, information is encrypted during the block cipher stage using a sub-key $Key1$, generated within the Key Generation block, and further encrypted at the physical layer by the Q4095 spreading code, seeded by $Key2$. This provides a robust level of security embedded within the signal design.

5.3.1 Waveform Architecture

Within this subsection, we outline the architecture of the overall Phorcys waveform, built upon the generic block diagram of figure 5.3.1, as depicted in figure 5.3.2.

The Phorcys waveform architecture, depicted in figure 5.3.2 (adapted from a version presented in [266; 6]), consists of a lower diagram half that represents the 'inner modulation codes' as well as a upper half that represent the 'outer spreading codes'.

These lower diagram illustrate how data packets are constructed through the concatenation of a frame sync waveform, an information-bearing modulation switch waveform, and multiple information-bearing data symbol waveforms. The concatenation of multiple data symbol waveforms forms the data payload section of the data packet, wherein the data undergoes encryption, representing the stream **x** as shown in figure 5.3.1. Additionally, this payload data is encrypted in accordance with $key1$ (the same as used in figure 5.3.1). The lower half's output represents the complex vector a, which is identical to a in figure 5.3.1.

The upper diagram in figure 5.3.2 illustrates how, once constructed, data packets are multiplied by an outer spreading code, thereby randomizing the inner information. This outer spreading code can either be fixed or securely generated in accordance with $key2$, serving to randomize the signal for both security and acoustic performance. In

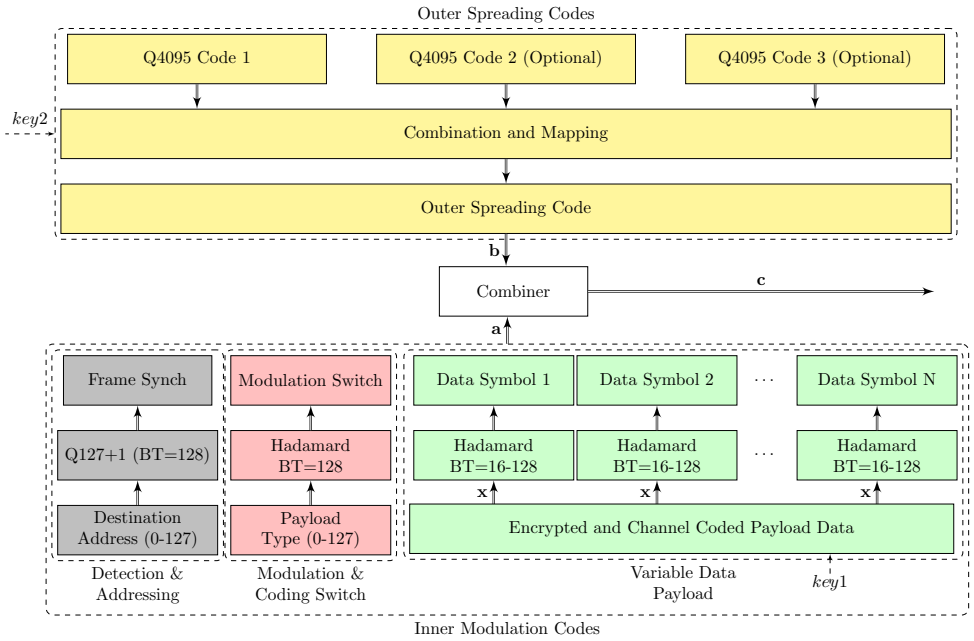


FIGURE 5.3.2: Phorcys Waveform Architecture

the latter case, the outer spreading code ensures that inter-symbol interference arising from long-duration multipath presents as uncorrelated noise to an adversarial receiver. The output of this upper half represents the complex vector b, identical to b in figure 5.3.1.

Both the outputs a and b from the inner modulation code and outer spreading code, respectively, are then combined, as discussed above, to form the vector c. This vector is subsequently mapped to the modulation scheme and transmitted. The Phorcys waveform architecture addresses key military end-user challenges in underwater acoustic communications (as outlined in section 5.1) across three distinct frequency bands chosen to cover disparate use cases: Medusa (less than 2 kHz), Euryale (8-12 kHz), and Stheno (20-28 kHz). The use of multi-band capability accommodates disparate end-user requirements that may be imposed by defence use. While the definition of distinct bands promotes the production of interoperable equipment, the Phorcys Physical layer has been designed to be arbitrarily scalable to any passband. This scalability was successfully demonstrated at the REP(MUS) 2021 trial, where the custom band 10-14 kHz was used in accordance with the trial transducer's capabilities. These distinct bands enable a variety of operational ranges and equipment capability sizes to be designed, ranging from shorter-range diver tracking systems to long-range towed acoustic transducers capable of travelling thousands of kilometres [267].

Within the defined bands, a number of 'gears' have been defined, offering variable performance depending on the channel conditions presented. The selection of these

gears is done by the network control plane in response to channel conditions and network performance metrics, further expanded upon in [97].

Frame synchronisation, modulation switch, outer spreading code, and data symbols are coded waveforms gain the benefits of direct sequence spread spectrum (DSSS), drawing from waveform sets featuring desirable correlation properties, based on either quadriphase or bi-phase construction. Frame synchronisation, modulation switch, and outer spreading code waveforms are based on quadri-phase sequences, and data symbol waveforms are based on orthogonal bi-phase Hadamard codes. The weak auto-correlation performance of Hadamard codes is addressed through the outer spreading code randomisation, and payload demodulator efficiency optionally optimised through the use of the Fast Walsh-Hadamard Transform.

In Phorcys, both modulation switch and data symbol modulation are based on an M-ary Orthogonal Signalling (MOS) technique [7], where information is conveyed by the transmission of one-of-M orthogonal waveforms, and the information is recovered at the receiver by correlating received waveforms against all possible waveform options. This realises log2(M)+P bits of information, where M is the orthogonal waveform set size, and P relates to the optional use of phase shift keying (PSK) to provide additional phase bits to increase bandwidth efficiency (MOS-PSK). Physical layer security is implemented jointly through key-based permutation of waveform mappings for frame synchronisation, modulation switch, and data symbols, and by multiplication of the constructed (frame synchronisation, modulation switch, data payload) data packet by the outer spreading code.

In Phorcys, frame synchronisation and modulation switch code lengths have been fixed at 128 chips to balance transmission brevity with detection/addressing and modulation switching robustness. Transmission brevity is motivated by the desire to convey addressing and modulation switching information robustly at a high tempo in multi-user environments. Data symbol code lengths are variable from 16 to 128 chips to provide a scalable data-rate/robustness trade-off, supporting low to medium data rate modes across short packet (2, 3, 4, 7 bytes) and long packet (16, 32, 64, 128 bytes) data payloads. SP modes are typically less than 100 ms (Stheno) in duration, aligned with tactical 'canned messaging' and navigation operational scenarios. LP modes, ranging from 100-4000 ms duration, align with text chat and compressed voice.

Initial detection and synchronisation of the DSSS frame synchronisation waveforms present well-known and understood challenges in acoustic signal design and processing (see, for example, [268; 269; 270; 271]). Within Phorcys coherent Stheno and Euryale bands, the narrowband Doppler tolerance of coherently detected frame synchronisation waveforms is a function of waveform duration and carrier frequency. Full decorrelation loss occurs when the Doppler Hz translation of the passband signal results in a full

carrier cycle over the frame synchronisation duration. One metric for Doppler tolerance is to assume half this velocity, i.e.,

$$v_d(\text{m/s}) = 0.5c[BW/(F.BT)] \tag{5.1}$$

Where (BT) is the frame synchronisation code Bandwidth-Time product. For the Phorcys Stheno band (BW=8kHz, F=24kHz, BT=128), it can be shown that v_d equates to just over 2 m/s or 4 kts, so additional receiver detection/synchronisation complexity is needed to support platform relative velocities exceeding this. The Phorcys specification does not prescribe technical means to extend Doppler tolerance beyond this limit nor does it prescribe receiver implementation around frame synchronisation detection processing and open/closed loop synchronisation methods. Narrowband and wideband Doppler tolerance of digital phase-coded waveforms and bounds on detection performance are developed in more detail in [268; 269].

Following detection and coarse synchronisation, the modulation switch waveform immediately follows the frame synchronisation waveform and encodes information using M-ary Orthogonal Signalling modulation. MOS is a proven and robust technique to convey $\log_2(M)$ bits of information in a single symbol interval. The MOS demodulator function and optimality assume waveform orthogonality is reasonably preserved against channel Doppler and multipath effects. The former is managed by the receiver's open-loop detection and coarse synchronisation function, and the latter is achieved by ensuring the modulation switch waveform coherent detection processing gain is both balanced with the frame synchronisation processing gain and sufficient to overcome channel multipath, noise, and multi-user interference impairments. In Phorcys, frame synchronisation and modulation switch are coherently detected DSSS waveforms, of length 128 chips providing PG = 10log(128)=21 dB, providing sufficient intra-chip fading margin for reliable modulation switch detection.

Simulations and field trial results [7] show the coherent modulation switch switching method to be resilient and robust down to the coherent frame synchronisation detection limit, which is typically in the region of -8 to -10 dB SINR (Signal to Interference Noise Ratio), depending on detection method. Here, SINR relates to noise contributions from multipath "self-noise" and/or background noise and/or multi-user interference.

In moderate SINR conditions, the wide-band character of the frame synchronisation and modulation switch waveform pair may be used to provide up to 256 chips (32 ms Stheno band / 64 ms Euryale band) of adaptive receiver training to condition modem physical layer in advance of demodulation. This includes, for example, receivers employing chip-level adaptive processing either directly through space-time adaptive processing (STAP) structures and/or indirectly leveraging the MOS-PSK waveform

design. Such structures demodulate at symbol level but adapt at chip level using a posteriori symbol decisions to drive the chip-level adaptation and synchronisation processes.

5.3.2 Waveform Capabilities

Interoperability and security are overarching priorities in the development of Phorcys, encompassing both physical layer security and broader information security components.

Physical layer security features build upon the core DSSS-based MOS-PSK modulation technique of the Phorcys waveform. This technique combines 'inner' information-bearing orthogonal codes with large dimension 'outer' spreading codes, providing joint transmission security and acoustic transmission resilience in challenging acoustic environments through the MOS modulation method.

The introduction of inner information-bearing codes in Chapter 4 delved into the characteristics of the Hadamard code. It explored the capability to transmit M-ary bits of information on a single codeword and demonstrated a novel method to retrieve bit-level LLR. The combination of the inner spreading code, with good cross-correlation, along with the outer spreading code, with good auto-correlation, overcomes some of the issues regarding time alignment and lag, as discussed in Chapter 4.

As discussed earlier in this section, security interoperability is achieved through the generation of both outer spreading code and inner code mappings based on a key generation component. These mappings include the frame synchronisation detection code (drawn from multiple families and cyclically distinct seeds) and symbol-to-waveform mappings used in the MOS modulation method. A more comprehensive description of Phorcys cryptographic security mechanisms is provided in the Phorcys Cryptographic Interoperability Specification [272].

Phorcys network interoperability leverages key capabilities provided by the secure DSSS-based waveform architecture, in conjunction with physical layer design and modem link layer protocol design. A key driver in the Phorcys waveform architecture design has been to minimise transmission duration while providing flexible support for future contention and non-contention-based media access control and networking protocols.

The Phorcys frame synchronisation and modulation switch waveforms (as shown in figure 5.3.2) provide these capabilities by utilising the MOS technique for addressing and modulation, respectively. Frame synchronisation offers a means for nodes to selectively detect packet transmissions based on waveform-level addressing.

Modulation switch provides a means for the modem receiver operating mode to be switched according to prevalent channel conditions and/or networking requirements. By binding destination addresses to specific frame synchronisation waveforms and mapping these waveforms to unicast/multicast/broadcast addresses, receiver modems can either admit or ignore in-water telemetry packets at the detection stage. This has benefits in crowded network environments since demodulating, channel decoding, and de-encrypting unwanted packets is not only wasteful of modem resources and energy but also risks modems failing to detect correctly addressed packets in crowded network environments.

The modulation switch waveform, immediately following the frame synchronisation, selects between multiple modulation-coding pathways, where each pathway can benefit from precision open-loop synchronisation/equalization/spatial processing/channel estimation opportunities afforded by the DSSS coded frame synchronisation and modulation switch waveform pair. Work is presently ongoing on Phorcys link and network protocols, with initial work reported in [97].

In summary, the frame synchronisation (detection) and modulation-coding switch waveforms are key underpinning components of the Phorcys waveform architecture, benefiting from brevity and DSSS coding processing gain, to provide resilient contention mitigation in respect of data packet destination addressing and data packet modulation mode switching. Network-enabling opportunities provided by the frame synchronisation and modulation switch waveform pair include enhanced data payload channelisation opportunities through time and/or frequency multiplexing via future data payload modulation and coding design flexibility.

Phorcys waveform environmental adaptivity relates to the ability of the waveform architecture to support range/resilience-data rate trade-offs depending on systematic and operational scenarios. The Phorcys modulation switch provides the means to switch between different modulation and channel coding pathways depending on environmental complexity and outboard array capabilities.

The current baseline Phorcys waveform specification describes variable-rate, MOS-PSK modulation modes in conjunction with two channel coding options. Short (2, 3, 4, 7-byte) packet data integrity is provided using a 16-24-bit Cyclic Redundancy Check (CRC) for error detection and a simple 'symbol flipping' algorithm for error correction, achieving a probability of undetected error (P_{ud}) less than 1×10^{-4}. Long (16-128-byte) packet integrity is provided using Reed Solomon (63,43) and (42,22) block codes with intrinsically lower P_{ud}.

Phorcys MOS-PSK bandwidth-time product (BT) adaption from BT=16 to 128 supports low to medium data rate modes from 10s of bits per second (bps) up to 1-2 kbps. Link rate adaption, using low-level MOS demodulator metrics and channel decoder metrics, is an area of ongoing development as part of the Phorcys Open Media

Layer architectural design and specification (POMLS) [266]. Work is progressing on enhanced single-carrier modulation adaptive receiver structures, which exploit MOS-PSK modulation symbol-level decisions to construct chip-level adaptive re-training sequences from demodulated MOS-PSK waveforms. Sequences are then used to update single/multi-element adaptive combining filters and closed-loop synchronisation aiding algorithms at each symbol step. The performance of these adaptive wideband receiver structures across a broader range of channel conditions is a current focus of work, alongside multi-element array design-complexity work [7].

The Phorcys DSSS coded frame synchronisation and modulation switch waveform architecture provides the means to flexibly introduce new data payload modulation and channel coding strategies, using and leveraging the frame synchronisation and modulation switch waveform capabilities to provide robust detection, destination addressing, and modulation-coding switching.

While MOS-PSK modulation is scalable to low to medium data rates, it is recognised that waveform extensions to support higher bandwidth efficiencies and/or means to provide improved data payload multi-user channelisation will be requirements of the future. It is anticipated that these high data rate (HDR) modes would operate within the Phorcys frame synchronisation and modulation switch DSSS coded MOS detection/addressing/switching 'umbrella' and leverage existing detection/addressing/switching functions to support such modes. The augmentation of higher bandwidth efficiency modes using MOS-PSK modulated short headers to protect vital link layer data (source ID, packet count, power management, etc.) provides means to achieve link resilience alongside more advanced channel coding and link management concepts (e.g. hybrid automated repeat request (HARQ)).

MOS-PSK short headers in advance of bandwidth-efficient modulation schemes can protect vital link layer information and provide means to undertake spatial-temporal adaptive training and/or channel estimation over longer delay spans to better accommodate channels with sparse, extended multipath structure. This applies equally to single-carrier and multi-carrier modulation modes as a means to provide enhanced channelisation in support of future networking concepts.

5.3.3 Waveform Performance

Within this subsection some performance of the Phorcys waveform, validated through sea trial activities, it is important to note that these trials were not conducted by the author of this thesis, and were conducted by collaborators at University of Newcastle and Sonardyne, and were presented in [7]; which was co-authored with the author of the thesis.

In January 2021, Newcastle University conducted recordings in the North Sea off the Northumberland Coast, UK, capturing Stheno and Euryale band signals at distances of up to 5 km and 20 km, respectively. The experimental setup involved a single omnidirectional hydrophone deployed at a depth of 7 m from an anchored vessel in approximately 30 m water depth (coordinates 55.146400, -1.420860). The transmitting system, featuring a linear power amplifier driven by a digital audio card, was transported to various distances in a southeast direction by a second vessel.

The Stheno band projector, deployed at a depth of 7 m, was driven to a sound pressure level of 180 dB re 1μPa @ 1 m. Simultaneously, the Euryale band projector, positioned at a depth of 14 m, was driven to an SPL of 186 dB re 1μPa @ 1 m. To facilitate a comprehensive analysis under comparable channel conditions, 100 short packets and 50 long packets were transmitted for each range and band, with the modulation gears interleaved.

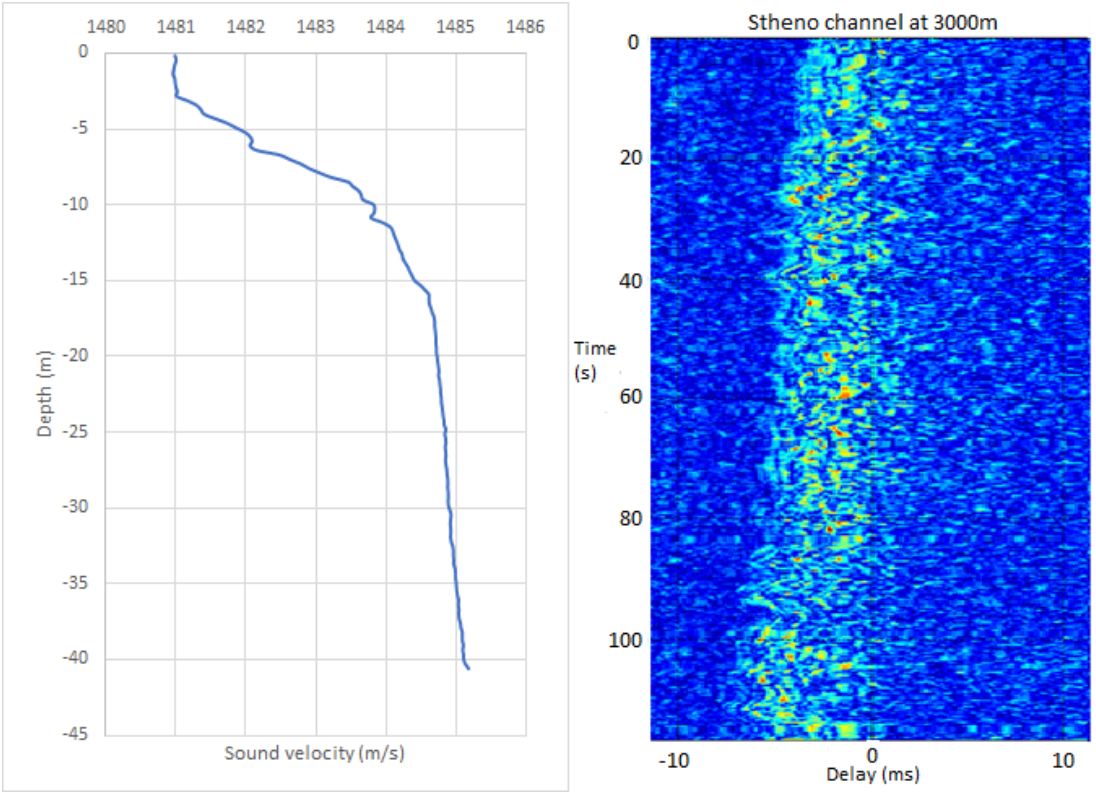


FIGURE 5.3.3: Sound velocity profile (left) and channel response for 3 km Stheno transmission showing time variability and slow drift of transmitter (right). From [7].

Owing to the cold weather and the increased flow of fresh water from nearby rivers, upward refracting, surface-ducted propagation manifested on the given day. This atmospheric condition, combined with the shallow deployment of the transducer, resulted in highly dispersive and rapidly time-varying channels at all ranges, posing a rigorous test for the waveforms. Figure 5.3.3 illustrates instances of the sound velocity profile alongside the temporal evolution of the impulse response. Marginally improved channel coherence is discerned in the Euryale transmissions, attributable to the lower

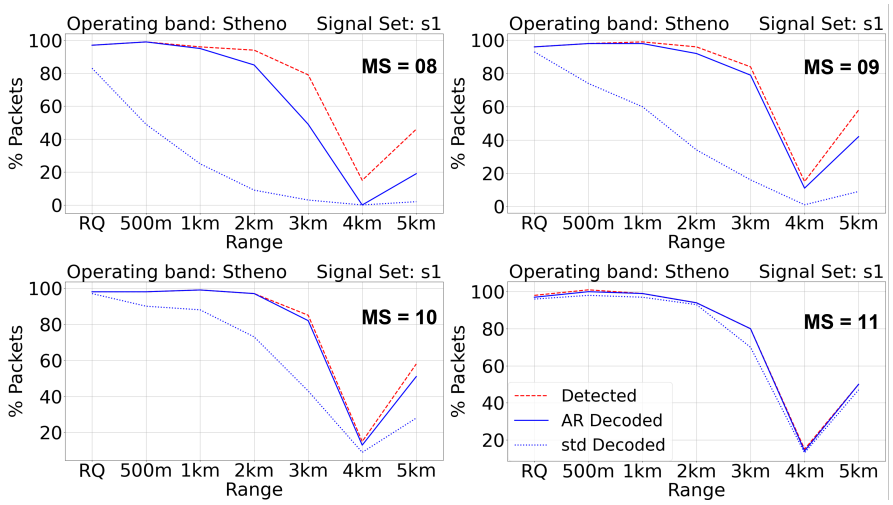


FIGURE 5.3.4: Packet detection and delivery rates vs range for North Sea transmission of short packet (MS 8-11) signals in Stheno band. From [7].

frequency and greater depth of the projector. The sound velocity profile was measured with a sound velocity probe at the site of the vessel, the probe analyses the water temperature, salinity and pressure and different depths in order to estimate the expected sound velocity profile [246].

Figures 5.3.4 to 5.3.6 present the packet (frame synchronisation) detection rate (depicted by the red trace) and packet delivery (successful decode) rate for a reference receiver (dashed blue trace) and an adaptive receiver (solid blue trace). Recorded ranges extend up to 5 km for the Stheno band and up to 20 km for the Euryale band (with "RQ" denoting a short-range test over 160 m in a nearby marina).

In figure 5.3.4, it is evident that for the highest BT gear (MS = 11), nearly all short packets detected are successfully decoded by the simple RC, but a notable decline in performance is observed as BT is reduced. However, the adaptive receiver demonstrates a substantial enhancement in delivery by leveraging more of the multipath energy. For the long packets, as depicted in Figure 5.3.5, the gain from the adaptive receiver is even more pronounced. This improvement is attributed to the adaptive receiver's capability to adapt to the highly variable channel, where a traditional receiver experiences fading of individual paths, along with superior phase/chip synchronisation. This is particularly evident with the MS=20 gear, whereby the adaptive receiver outperforms the reference receiver by a significant margin, whereby the adaptive receiver can decode messages up to and beyond 3km, approaching the performance of the detection waveform. This is in comparison to the reference receiver which suffers poor performance above 1km.

Figure 5.3.6 illustrates how, in the Euryale band, with a slightly more favourable channel response, the adaptive achieves near 100% packet delivery in almost all gears and ranges, constrained only by the upper bound of frame synchronisation detection.

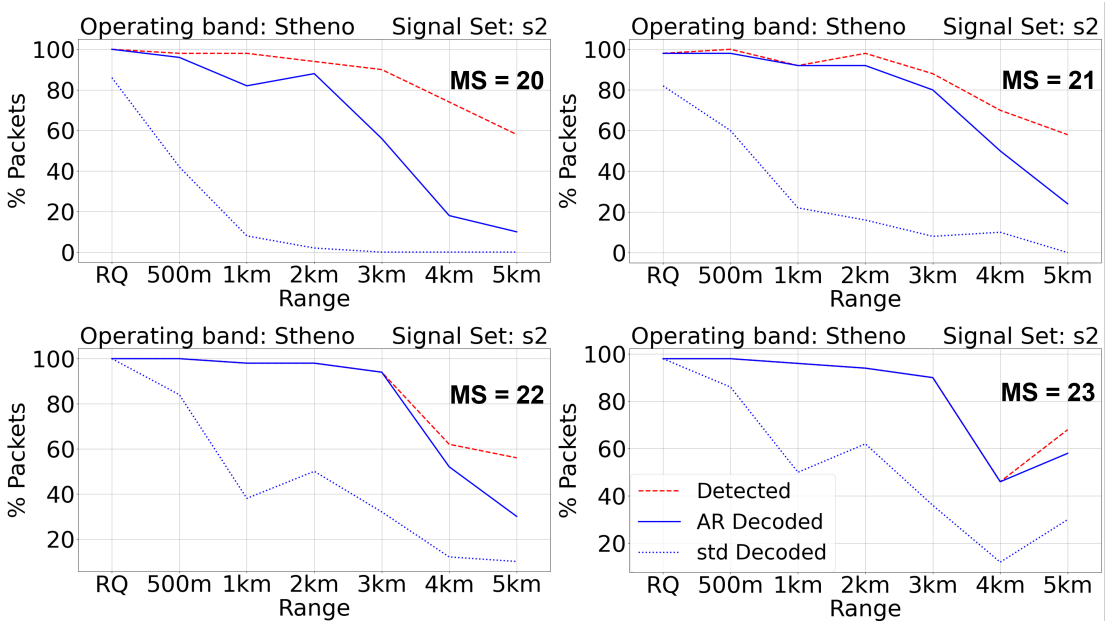


FIGURE 5.3.5: Packet detection and delivery rates vs range for North Sea transmission of long packet (MS 20-23) signals in Stheno band. From [7].

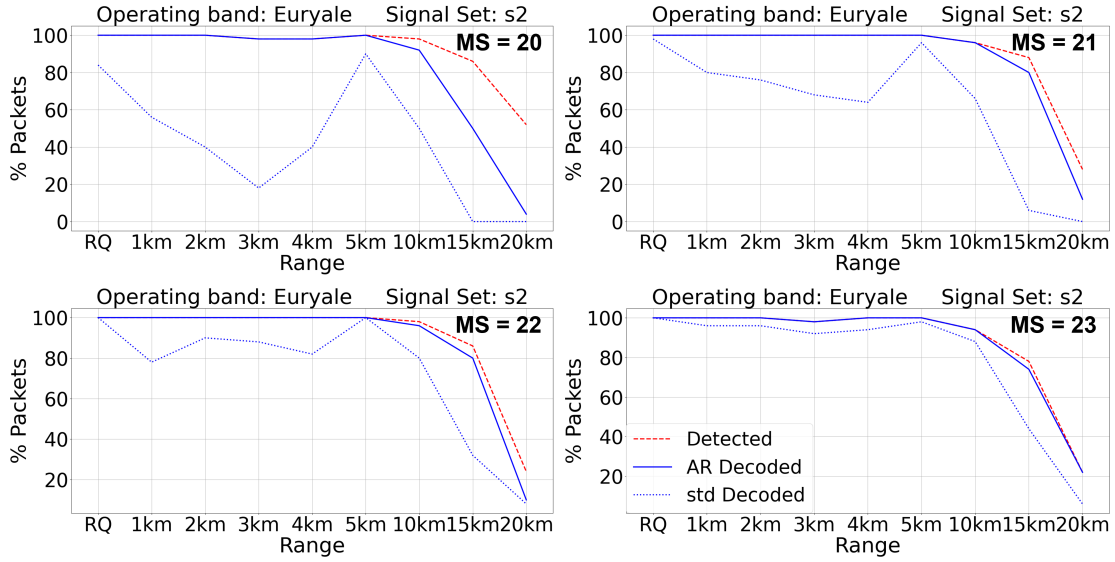


FIGURE 5.3.6: Packet detection and delivery rates vs range for North Sea transmission of long packet (MS 20-23) signals in Euryale band. From [7].

The adaptive receiver used to generate these results is discussed further by collaborators in [7] and [273].

The performance of these waveforms, although they have not been directly compared against the JANUS standard yet, are expected to have similar or superior performance in terms of range, as can be seen when the results above are compared to [245] whilst significantly reducing the amount of transmission time. The JANUS packet length is of the order of 2.1s whilst Phorcys is of the order of a couple of ms. This significant improvement (over 100x) in timing efficiency not only reduces the power usage, but also reduces the impact to marine life and improves spectrum utilisation for networked scenarios.

5.3.4 Secure family of Waveforms

Phorcys has been developed as a ”secure-by-design” open standard (pending ratification), inheriting foundations from other security techniques by building on AES, SHA, and other established security protocols. Furthermore, Phorcys has been developed as an open standard. Open standards reject the fragility of security by obscurity and are vital for enabling international interoperability. They also facilitate natural open competition for compliant products, supporting users to receive better implementations, similar to the approaches in 3GPP [148] and 802.11 for developing 5G and WiFi.

The security of Phorcys manifests as both Communications security, which protects data through encryption, and physical layer security, obfuscating the waveform where confidentiality, integrity, and authentication are provided by a pre-placed key. This is achieved with only lightweight processing overhead, without adding contextual security data to the packet, preserving the available message payload. The security aspects of the physical layer of Phorcys can be described as follows:

1. **Encryption:** Data from higher layers (including the Link layer) is encrypted based on its payload size. ”Short” packets use a substitution table for encryption, with block mixing achieved by combining the lightweight SipHash with the substitution table in an unbalanced Feistel network [274]. ”Long” packets use ”wrapped” AES [275]. Wrapping and block mixing ensure that any change to any plaintext in any block affects all blocks in the packet, making semantic cryptanalysis more challenging;
2. **Inner Modulation:** The bitstream is organised into symbols, mapped to chips derived from rows of a Hadamard matrix. This mapping is obscured by the key;
3. **Outer Spreading:** The chips are spread using a non-linear combination of Linear-Feedback Shift Registers (LFSRs), improving packet detection

performance by decorrelating the packet with multipath components of itself. These codes are derived from the key and have optimal correlation properties, making Phorcys easy to detect in noisy environments for someone who knows the key, and difficult to detect for everyone else as the packet appears as noise.

The security of the Phorcys communication protocol is reinforced by the inherent properties of Hadamard codes. The multiplication of one Hadamard code with another results in yet another Hadamard code [276]. This mathematical property adds a layer of complexity to the bit stream, making crypto-analysis challenging. The intricacies of the Hadamard mapping functionality remain obscure to an adversary, as the relationship between the transmitted and received codewords involves complex operations that are not easily deduced from the bit stream alone. This characteristic enhances the protocol's resistance to cryptanalysis, contributing to the robustness of Phorcys in secure underwater communication applications.

A further element of scalability, Phorcys inherits the concept of an epoch from Venilia, discussed further in Section 5.4.4 and [5; 2]. In Phorcys, the epoch changes how frequently spreading codes, mappings, and encryption keys change, resetting any cryptographic knowledge determined by an eavesdropper; determining a spreading code in one epoch does not support any crypto-attack in the next. Phorcys uses derivations of the pre-shared key rather than the key itself, so this key does not need to change each epoch. This does not imply tight time-synchronization between two devices; epochs can be of the order of minutes, hours, days, or even longer, and the time-synchronization requirements scale linearly in roughly equal order of magnitude.

Phorcys inherently supports networks of up to 128 addresses with specific protocols in development for mesh and linear network topologies. Short and long packets have both been successfully received from in-service platforms with further trials planned [2].

5.4 Security Techniques

Within this section, we explore concepts to enhance security and introduce a novel method to incorporate security into the existing NATO standard for underwater communications.

5.4.1 Traditional Security Approaches

Especially for military users, ensuring the confidentiality, integrity, and authenticity of information is a key requirement. Confidentiality is typically achieved in traditional above-water systems by using cryptographic algorithms to encrypt data at the source

and decrypt it at the destination using a key. The most common cryptographic algorithms fall into two categories:

1. **Block Ciphers:** Examples include AES [277] in block cipher modes.
2. **Stream Ciphers:** Examples include ChaCha [278] or block ciphers in stream cipher modes, such as Galois Counter Mode (GCM).

However, challenging underwater conditions and long latencies in the acoustic channel drive bit rates below optimal ranges for standard cryptographic security techniques. This motivates the development and application of algorithms specific to the underwater use case.

5.4.2 Block Ciphers

The widely used block cipher, AES [277], has a block length of 128 bits, meaning that this is the smallest number of bits the algorithm can work with. Any data packet with a length less than 128 bits must be padded with dummy data to fill the difference. A standard baseline JANUS packet contains only 34 bits of data [118], requiring an additional 94 bits of padding to be transmitted by extending the packet payload. In this case, the 34 bits of user data would make up only 27% of the transmitted data—a significant inefficiency in the already limited underwater channel.

5.4.3 Stream Ciphers

Stream ciphers do not have a minimum length requirement, eliminating the need for additional padding of transmitted data. Encryption is performed by generating a key-based pseudo-random sequence K and applying the XOR operation, addition modulo 2, bitwise on the plaintext P to generate the ciphertext C, such that $C = K \oplus P$.

However, there is a strict requirement not to encrypt different plaintext messages P_1, P_2 using the same keystream K, as this would allow an observer to recover both the message and part of the keystream. Reuse of the keystream can be avoided by either changing the key frequently enough so that every message uses a new key or by including an Initialisation Vector (IV) that changes for every packet encryption. There is no need to keep this IV secret.

The long propagation delays inherent in underwater acoustics, due to the relatively low speed of sound in water, make the frequent key update approach impractical, as the key may change before the message arrives successfully at the destination. This would

mean the key used at the receiver to decrypt the message would be different from the key used at the transmitter to encrypt the message, leading to decryption failure.

Including an IV as part of the packet would avoid the need for frequent key updates but would add additional overhead, reducing the amount of useful user data that could be transmitted. The number of times a key can be reused securely is proportional to the exponent of the length of the IV, so long-duration keys would require more bits to be allocated to the IV. However, when there are no strict constraints on the message length or data rate, sending an IV may not be as problematic, as discussed in [1].

Therefore, this method may be challenging to apply in the underwater domain, especially for low-power devices such as sensors and diver communication systems, where data rates are low, and such overhead would be prohibitively inefficient.

Nonetheless, ensuring secure communication in underwater acoustics poses challenges, particularly in addressing the requirement to avoid encrypting distinct plaintext messages, P_1 and P_2, with the same keystream K. Such repetition could enable an observer to compromise both the message and a portion of the keystream. Common strategies to prevent keystream reuse involve frequent key updates or the use of an Initialisation Vector (IV) for each packet encryption. The former proves impractical in underwater scenarios due to prolonged propagation delays, potentially resulting in the key changing before the message reaches its destination. The latter, employing an IV, introduces additional overhead and may not be ideal for scenarios with limited data rate or strict constraints on message length. This difficulty is exacerbated in the underwater domain, especially for low-power devices like sensors and diver communication systems, where efficiency is paramount, and transmitting an IV may be impractical.

Several proposals for ensuring security in the underwater domain are presented in the following sub-sections, where the novel schemes of Venilia and Phorcys Cryptographic Interoperability Specification (PCIS) are introduced.

5.4.4 Integrated Physical Layer Security

Phorcys has been designed to provide inherently secure communications: the specification itself is open, but the user defines the keying of security functions of the protocol. The secrecy of the key, its transportation and generation ensure a high level of information security, informed by the collective white-hat cryptanalytic efforts on the constituent open standards.

Security in Phorcys is provided by Phorcys Cryptographic Interoperability Specification (PCIS), which enables interoperable security in pre-placed key networks. A key feature of PCIS is the optimisation of security with zero data overhead, by

leveraging implicit information according to (macroscopic) time or spreading codes. By taking such an approach, PCIS uses the properties of the underwater channel to enable security, in contrast to traditional algorithms which may be severely limited by the constrained channel.

A master key is at the core of assigning sub-keys for various functions in the physical layer. These functions include tasks like Hadamard code mapping, Q4095 sequence generation, and generating an AES 256-bit key. The sub-keys are created by applying a hash function to the master pre-placed key along with knowledge of the current time epoch (user-defined time epoch, based on risk analysis of the operation). The mapping of the keys can be seen in figure 5.3.1. This straightforward process ensures the consistency and security of the sub-keys, establishing an effective and secure system for deploying cryptographic elements across the protocol. The use of a hash function adds to the protocol's reliability by providing a secure way to generate sub-keys from the master key, strengthening the overall security of the communication system.

In the Phorcys communications protocol, using subkeys has a practical advantage. Connecting a subkey to its main master key through a hash function adds a layer of security. If a subkey is compromised, it doesn't jeopardise the entire master key. This minimises the risk of a major security breach. The approach ensures that the pre-placed master keys can still be used securely without compromising the overall security of the protocol. In essence, this provides a pragmatic way to enhance security and maintain effective communication.

PCIS outlines a holistic approach to security, covering techniques for communications security to provide confidentiality and integrity, and physical layer security to protect the signal in transit and provide both availability and authentication. Both approaches are based on the use of a 256-bit symmetric pre-placed key, a level of security widely used for public and defence scenarios. Further details are outlined in [5], including the motivation for and details of the enhanced security design.

5.4.5 Venilia

When transmitting only the JANUS baseline packet with no cargo data, the usage of traditional block ciphers such as AES-GCM is not practical, and a different strategy needs to be used to encrypt the information included in the application data block (up to 34 bits).

To address this issue, the Venilia class has been developed, which is an enhancement to JANUS that addresses the need for interoperable, secure, low-latency underwater messaging [279]. Defined as an additional *User Class* of JANUS packet, Venilia specifies the content and format of the standard 34 bit data payload, bits 23 to 56, to

include 8 bits of user data and the remaining 26 bits for network addressing and validation [1]. The structure of Venilia is shown in figure 5.4.1.

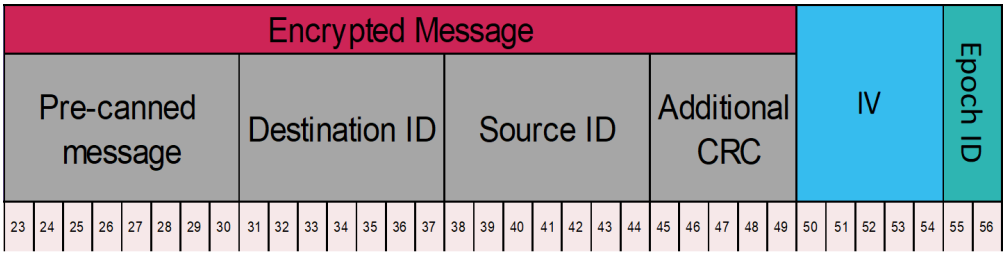


FIGURE 5.4.1: Venilia bit structure, as part of the larger 64-bit JANUS packet, containing an 8-bit pre-canned message, source and destination IDs, 5 bits of Cyclic Redundancy Check (CRC), a 5-bit IV, and 2 bits as a time epoch flag.

The core component of a Venilia packet is an 8-bit integer that represents one of 256 (2^8) possible messages that have been pre-agreed by users, known as pre-canned messages. This provides a data-efficient method of exchanging information, acting as a form of compression for user data to minimise the required packet length, and so reduce the time energy is transmitted through water. Along with the user data, the network address of the sending node and chosen destination address are included, each represented by 8-bit values and 5 bits of cyclic redundancy check to detect any changes to the data in transit and verify the integrity of the message. The CRC is based on the International Telecommunications Union Cyclic Redundancy Check (CRC-5-ITU) and is defined by the polynomial $z = x^5 + x^4 + x^2 + 1$ [280].

Combined, the pre-canned message, source and destination network addresses, and CRC total 27 bits, which are encrypted together using TUBCipher (Tiny Underwater Block Cipher), a novel ultra-short block-length cipher described in Section 5.4.5.1.

An epoch is a period of time of a fixed duration known implicitly to every device on a network, that acts as a nonce (number used once) for the encryption algorithm, so that the same plaintext produces different ciphertext if encrypted in different epochs. It is ordinarily based on system or Unix time. The least significant two bits of this 32-bit variable at the time of encryption define the Epoch Identifier. Epoch Identifier uniquely resolves the ambiguity of the receiver in which epoch was used to encrypt a message.

An initialisation vector (IV) of 5 bits is included as part of a Venilia packet to reduce the viability of frequency analysis attacks on the encrypted payload. The IV should be updated after every message in an epoch, such that no two messages are encrypted with the same IV in the same epoch.

[1] Venilia is specifically designed to encrypt the content of the JANUS application data block and may be less efficient when applied to long messages (e.g., JANUS cargo) for which AES-GCM can be used.

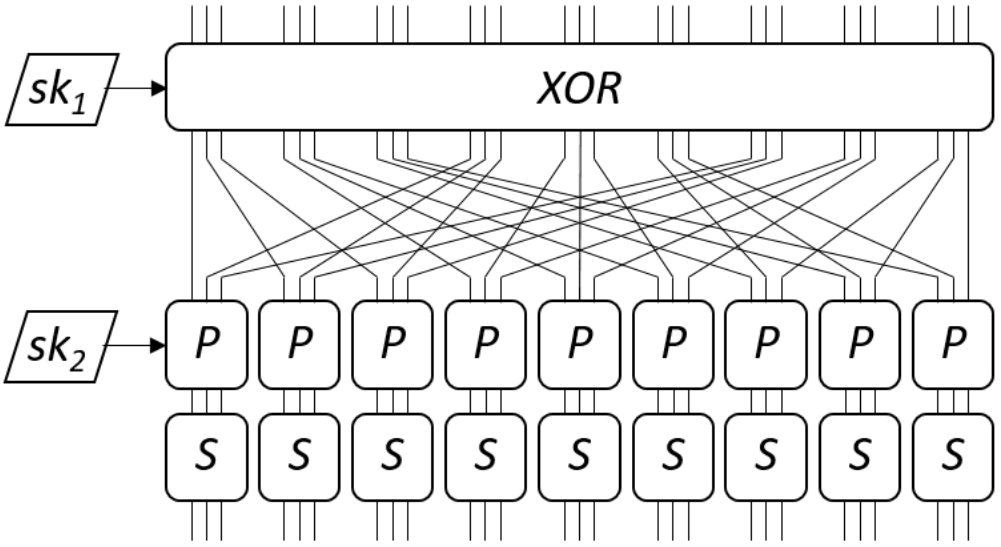


FIGURE 5.4.2: Bit mapping and basic round structure for one round of TUBCipher. Subkeys sk_1 and sk_2 change for each of the 56 rounds

5.4.5.1 TUBCipher

TUBCipher is a substitution-permutation network, a common type of block cipher, producing 27 bits of ciphertext from 27 bits of plaintext [281]. TUBCipher was built by accepting generalisations to PRINTcipher, a pair of block ciphers built for printing on integrated circuits for applications such as radio frequency identification (RFID) tags [282]. TUBCipher expands PRINTcipher in accordance with the former's higher power applications, using independently random, distinct exclusive-or operations for each of its 56 iterations. This independence of "subkeys" - generated by cryptographically mixing the epoch and IV - from one round to the next prevents a viable type of cryptanalysis called a slide attack, an attack that focuses on weak or predictable key schedules.

The round structure of TUBCipher is given in figure 5.4.2. TUBCipher's similar architecture ensures it inherits much of the security analysis of PRINTcipher; and by extension, the resilience of Venilia to some common cryptographic and communications exploits, including spoofing.

However, this work is just encryption; while encryption of Venilia's CRC gives some tamper protection, the link itself is still vulnerable to eavesdropping and semantic analysis by an attacker. Future generations of underwater acoustic communications require protections for the packet, not just the payload.

5.5 Integration with Autonomy

This section provides a systems-level view of how underwater acoustic communications and autonomy can work in unison to achieve overall mission goals, as defined by an

end-user requirement.

It builds upon the previous sections and starts to present concepts of how underwater communications can work within an autonomy framework to position autonomous platforms best within the underwater acoustic environment.

Technology in the underwater domain is rapidly increasing in capability, with ever-developing robotics technology enabling a wider variety of actors to access the subsurface domain. This has facilitated a significant increase in capability that can be provided for underwater missions. One of the key challenges to overcome given the increased appetite for underwater missions supported by robotic systems is underwater communications. It has long been recognised that any form of communications is difficult underwater [283; 284] and there is a severe trade-off between range and achievable data rates, primarily due to the transmission medium and its variability with time and location [285; 286]. Acoustic communication is the most common medium choice and is the only method for communicating over more than a couple of hundred meters. Most underwater nodes (whether they be static or mobile) will be outfitted with an acoustic modem, with some also receiving an RF or optical modem too. Recent efforts have led to the deployment of networks of these nodes, usually networks of seabed sensors communicating data to a surface station. Much prior work exists on how these underwater communications networks can be used to support autonomous behaviour [287; 256], but this section presents a different viewpoint: how can the communications networks and the autonomous behaviours interact together to maximise the mission effectiveness. While most of the previous literature has focused on using communications to enable cooperation of AUVs, this work aims at proposing a tighter relation between autonomy and communications, so that, for example, autonomous behaviours can also be used to support communications.

Underwater Acoustic communications are typically limited in range and coverage by the ocean conditions in which they exist; furthermore, they are often utilised to support AUV) operations. Within underwater acoustic channels, one of the biggest considerations for whether communications can be achieved is the environmental parameters, such as bathymetry or whether an acoustic line of sight exists between two nodes. The use of autonomous vehicles presents an opportunity to adapt the physical network topology to these environmental parameters. Unlike traditional networking infrastructure, AUVs are mobile platforms and could be tasked to position themselves to support a communications infrastructure.

In order to provide motivation and context for this work, this chapter presents two use cases in section 5.1. They have been sourced from military requirements for dynamic underwater networks but are representative of a much wider variety of uses. Towards the end of the section, work is presented on creating more modular and interoperable

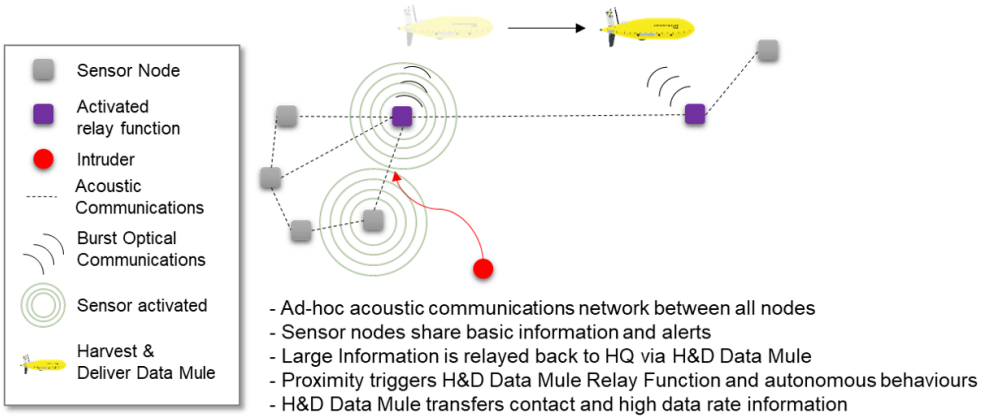


FIGURE 5.5.1: Concept of an autonomous Harvest and Deliver data mule

systems, a key enabler for the widespread usage of the novel techniques described in the earlier sections.

If communication networks could be optimised to their environment (in terms of the location of the nodes) to support efficient communications across the entire network, there is potential to significantly improve performance (e.g. in terms of robustness, throughput, and delay) over existing pseudo-static networks. In this section, we review and propose methodologies to make this ideal situation a reality.

5.5.1 Data Mules

To augment the capability of the proposed underwater acoustic systems further, due to limited and range-dependent bandwidth of underwater acoustic systems, it is useful to understand how data may be carried submerged throughout the network as a totality. To this end, it is useful to introduce the concept of a data mule; whereby it is beneficial to have high-latency but (relatively) large amounts of data transfer.

At a simplistic level, a data mule may be considered to be physical media storage moving data between two spatially separated network nodes. This type of data mule may also be described as a harvest and deliver data mule as it is harvesting data from one physical area of the network to deliver it to another.

Breaking the concept down for underwater networks, this creates 5 distinct phases, which are described below:

1. Hailing of the Data Mule;
2. Initial Flight to Information Source;
3. Information Upload;

4. Flight to Information Sink;
5. Information Download from Data Mule.

Where the total transmission time can be described in (5.2)

$$T_{\text{total}} = T_{\text{hailing}} + T_{\text{initial flight}} + T_{\text{upload}} + T_{\text{flight}} + T_{\text{download}} \tag{5.2}$$

5.5.1.1 Hailing

During the hailing phase, the data mule must be hailed to the information source. This must occur with a robust, reliable, and reasonably long-range, but potentially low data rate underwater communications bearer; as such, this task lends itself to underwater acoustic communications.

During this stage of hailing, the authentication of the information source by the data mule must be a top priority, to ensure that the data mule travels to a trusted node; and appropriate security measures must be applied [288].

5.5.1.2 Initial Flight

Once the Hailing stage has completed, and the data mule has been correctly identified by the information source, and the data mule has authenticated the information source, which requires the data mule, then the data mule must navigate to a position whereby it can utilize a high data rate communications medium to initiate upload to the data mule.

During this initial flight, the data mule will come under the command and control structure of the information source, and as such, must be able to remain in communications and situational awareness with the information source.

5.5.1.3 Information Upload

Once the data mule has arrived at a physical location whereby a higher data rate communications medium may be able to be used to transmit a large amount of data, the information upload can occur. During this stage, a suitable level of link encryption can be utilised to ensure appropriate security goals can be achieved.

An optical communications bearer is the most appropriate choice of communications during this information upload, proving data rates (during the upload) potentially in excess of 1 Gbps. Several potential options are discussed in [289], and a practical

system that can be utilized off the shelf will likely provide somewhere in the order of 10 Mbps, such as the Sonardyne BlueComm 200.

5.5.1.4 Flight

Once the Information content has been safely loaded onto the data mule from the information source, then the Data Mule must travel to the end destination, or information sink. It is imperative that during this flight, the data mule plots appropriate coordinates to ensure safe passage but also remains in some form of communications with the information source until an appropriate hand-over of command and control can be achieved. This is to ensure that the Data Mule can identify another node of any issues in flight, as well as providing another node with situational awareness of the location of the data mule.

5.5.1.5 Information Download

Once the data mule arrives at the information sink, the information needs to be downloaded off the data mule. An appropriate authentication process will need to occur between the Data Mule and the AUV to ensure that the information being downloaded is from the true information source, and also to ensure that the information sink is the true recipient and not an interceptor.

The information can then be downloaded, either by the physical retrieval of the information content via wired means or likely by optical communications if both assets are submerged.

Whilst the data mule concept is attractive for sending large volumes of data with high latency, it must be remembered that the overall data rate of the holistic system is determined by a number of factors. If we take into account the total transmission time within (5.2) then it is possible to define the overall Data Rate as (5.3).

$$\text{Data Rate} = \frac{\text{Data Packet Size}}{T_{\text{total}}} \tag{5.3}$$

This data rate in practice could, in fact, be less than some of the low data rate protocols that are observed in underwater acoustic Communications; thereby, as part of the overall mission planning, these factors should be considered before employing such a data mule.

5.5.2 Autonomy and Communications

The previous sections described the main challenges of underwater communications and possible ways for autonomy to support communications. From an autonomy perspective, communication requirements can be integrated into the vehicle's on-board control system following two different conceptual methods, and each method has a direct influence on the ability of the vehicles to balance mission requirements with their communication needs. In most cases, the main reason why an AUV is deployed is to collect data, and communication grows in priority based on the importance of the collected data itself. For example, in an ASW scenario, there is no need for the vehicles to continuously communicate unless a possible object of interest is detected.

In the typical approach, the communication and autonomy layers are separated. The autonomy system uses communications mainly to share data with other vehicles or nodes of the network and/or with the command and control center. The autonomous decision-making process is rarely communication-aware, which means that mission-level decisions or the vehicle trajectory planning are only based on the overall robotic mission goal. When communications are included in the autonomy framework, they are often seen as additional planning or bandwidth constraints. Vehicles might be requested to stay within a predefined communication range [290; 291], or, as in the case of gliders, to periodically surface to get radio or satellite communications, or their trajectory is planned so that they can pass close to gateways and/or communications relays to offload data or update their mission parameters.

For example, [292] proposes to include communication constraints through rendezvous points to address communications limitations of mine countermeasures scenarios. In this case, the vehicles dynamically agree on a meeting point to exchange target locations, to decide how to allocate remaining and new tasks, and to agree on the next meeting point and location. The disadvantage of this method is that vehicles are only guaranteed to be in communication at the rendezvous points. This limits in-mission collaboration and loses resources as the vehicles have to travel to the rendezvous points.

5.5.3 Modular Communications Architecture

To address this current lack of standardization, a modular communications architecture is proposed. This consists of a set of well-defined software interfaces between each layer of the communications stack. Any new implementation of these layers would simply need to implement the defined interfaces and could then be swapped into the stack. The rest of the system should be completely ambivalent to the change. In this first proposal, the OSI 7 layer model is used as a reference communications stack; however, it is recognized that underwater communications are sufficiently different from terrestrial communications to potentially warrant a

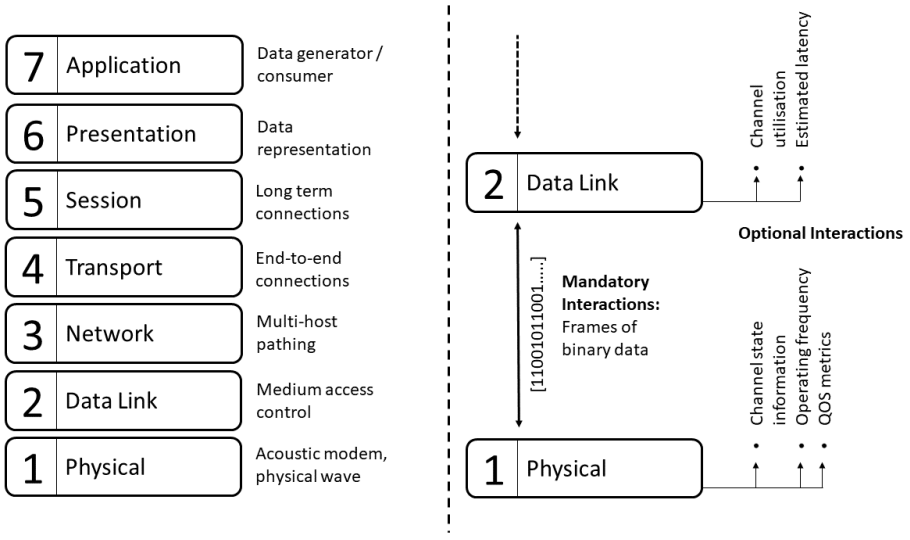


FIGURE 5.5.2: The OSI 7 layer model, with a brief description of the service offered by each layer, further showing the minimum, and optional, interactions between the last two levels of the OSI stack in the context of underwater communications

compressed version of this stack. Due to the low bandwidths typically available in the underwater domain, the benefit of additional stack layers may be outweighed by the additional message overhead. For example, in the OSI stack layer 5 and 6 are placed within the application layer - it is the application's responsibility to maintain sessions and handle data representation. The OSI model is briefly presented in figure 5.5.2 Layers 1, 2, and 7 are key requirements for any communications network, with layer 3 required to support multi-hop networking and layer 4 potentially useful for end-to-end quality of service provisioning.

This interface should include the core functionality of each layer. As an example, take layers 1 and 2 of the OSI stack. The only required interaction between the physical and data link layer is the exchange of the data packets that have been received or need to be transmitted. Therefore, a standardized interface between these two layers only needs to include functionality for passing these packets. Each layer will require a slightly different input to achieve core functionality; for example, the network layer requires both data and a destination address as an input. This concept is similar to the Cognitive Communications Architecture (CCA) developed by the CMRE [116]; the CCA also splits communications into several well-defined layers. The layers in the CCA are based on the OSI stack, and the system has been trialed several times by the CMRE, with favorable results. The architecture proposed here is in many ways a simplification of the CCA, so its success is taken as a good indication.

If the core functionality of a modem were to be wrapped up in the physical layer interface, the process of installing a new modem could be made relatively painless. A member of the community (or the manufacturer themselves) would need to develop this small driver, and then it could be spread around the community. As long as it

correctly implements the common upwards facing interfaces (i.e. the interface facing the data link layer is maintained), then it should work seamlessly on as many platforms that have adopted this architecture. Potentially this could be taken a step further, with control of the modem being further abstracted away from the physical layer and placed into a dedicated modem driver layer. This would allow the physical layer to concentrate on modem-agnostic issues, such as estimating channel state.

Each level of the stack has a minimum amount of data needed to function; however, it is clear to see the benefit of exposing other (optional) information for the system to make use of. For example, the physical layer is in the best position to infer metrics on the channel state, and the network layer may be able to maintain a topography of the locations of devices in the fleet. Utilizing a well-defined interface to share this information with the rest of the system would enable better modularity while maintaining some flexibility. An example of the mandatory and optional data types on layer 1 and 2 of the OSI stack is shown in figure 5.5.2b.

This functionality is a central building block of this architecture but has important design implications. On a typical operating system, the lower levels of the communications stack are buried within the kernel, only accessible through system calls. Developing kernel modules is no simple task; this requirement would severely limit the accessibility of this solution. Kernel modules also require system-dependent compilations, and multiple versions may be required to compensate for differences in hardware.

A final consideration is that each interface in the architecture should be 'push-centric.' The stack modules should not need any prior knowledge of the internal configuration; things like bus data rates should be hidden. Instead, each module should be free to push as much information as it can generate.

The drive for more modular underwater systems is not unique to the communications methodologies. The backseat control architecture proposed in [293] isolates the platform-dependent dynamic control systems from autonomous behaviors. The architecture offers an interface to abstract the platform control, allowing for significant code reuse. Indeed, as a model for underwater vehicles, it has gained significant traction in the community. The architecture proposed in this section can be viewed as an extension of this idea, placing the communications stack into the backseat.

This is not a reinvention of communications standards. Rather it is an approach to simplifying the way they are implemented into systems. The architecture proposed here sits firmly within the operating system and abstracts away the details of the individual communications protocol into a series of system calls. Some manufacturers already provide such a library, but this architecture aims to be flexible enough to encompass all of these into a shared interface.

5.6 Standardisation Activities

Standards are crucial for enabling different nodes of a communication system to interpret the intended message in a multi-vendor, multi-operator environment. This allows nodes to take appropriate actions, such as moving a vehicle, responding with another communication, rebroadcasting a message, or any other possible actions.

This requirement is universal for all communication systems and needs to be transmitted efficiently within the environment where communication nodes exist to reduce the energy of any given transmission. Specifically, the Energy Power per Bit, commonly referred to as E_b [2]

Currently, nations may choose to use NATO Standardisation Agreement (STANAG) 4748 ed. 3, known as JANUS [118], to provide a level of interoperability. There are associated limitations with JANUS, and in [294], some options were proposed for modifications to JANUS; however, to date, none have been ratified to the standard.

A JANUS Support Team has been proposed by interested NATO nations to track these modification proposals, such as new frequency bands proposed by the European Defence Agency (EDA) SALSA project or the Venilia class specification discussed in section 5.4.5 [244], which may aid in the development and acceptance of these modifications.

It would be remiss to discuss standards for underwater communications without mentioning JANUS [118], which is the current extant digital underwater communications standard[3]. JANUS is currently undergoing development beyond its current variation, as it is felt by some user nations that the current protocol is not fit for purpose due to its inefficiencies in design, lack of security, and lack of inherent networking capability.

JANUS will be further discussed in the following subsections, where a brief discussion is provided on the relative merits of current and potential future standards for underwater communications.

5.6.1 Extant Standards

Within this section, we provide an overview of the extant standardisation activities within NATO and discuss some pertinent aspects related to them.

[2] In this context, a 'Bit' typically refers to one of the binary bits after going through the channel coding process, see Section 2.1.2. However, a more accurate representation would be to refer specifically to information bits.

[3] There also exists a standard for Underwater Telephone, which is a single-sideband voice communications system but is an Analog communications scheme.

The current NATO underwater communication capabilities are standardised as follows:

- STANAG 1475 (old 1074 and 1298) - analogue tactical and safety communication between operators;
- STANAG 1481 - Identification of Friendly Submarine (IFS - ASIP-01) for the digital secure and covert communication stack from the physical layer to the military application layer for manned and unmanned submerged vehicles;
- STANAG 4748 (JANUS - ANEP-87) - open digital communications.

The IFS is classified as a NATO SECRET standard and is not allowed to be used outside of highly classified NATO environments. Hence, this section concentrates on JANUS, which is an open standard and facilitates research outcomes without any bureaucratic restrictions.

JANUS is the first and (as of today) the only open standard for digital underwater acoustic communications. Its bit allocation table and signal modulation are described in [295], and a reference implementation is freely available with an associated GPLv3 license online [296].

Figure 5.6.1 shows a time-frequency representation of a JANUS packet, taken from [118], where the frequency hopping nature can be clearly observed.

Three (optional) ”wake-up” tones are followed by the detection preamble, which is a 32-bit Binary Frequency-Shift-Keying (BFSK) modulated sequence. Then, there is a message of 64 bits that is mapped into a 144-bit Frequency Hopping BFSK (FH-BFSK) modulated sequence. These 144 bits define the ”baseline” JANUS packet. Depending on the message type, 34 bits (application data block) out of 64 bits is the maximum data size that can be used in the baseline packet. If more data is required, a ‘cargo’ signal of arbitrary size can be appended to the baseline packet using the same FH-BFSK modulation. The JANUS waveform has been designed to be scalable in frequency, with all parameters being ratiometrically calculated from the center frequency. A center frequency of $11,520$ Hz is chosen, resulting in a frequency band between $9,440$ and $13,600$ Hz and in a bit rate of 80 bps.

The key characteristics of JANUS are its simplicity of implementation and its ability to cope with noisy and highly reverberant channels. During the past six years, JANUS has been extensively demonstrated in various applications such as transmission of the automatic identification system and meteorological and oceanographic data to underwater assets, in distressed submarine scenarios, and for the exchange of short text messages [297].

As originally designed, JANUS had no provisions for native and built-in security aspects. However, the content of a JANUS packet (both cargo payload and application

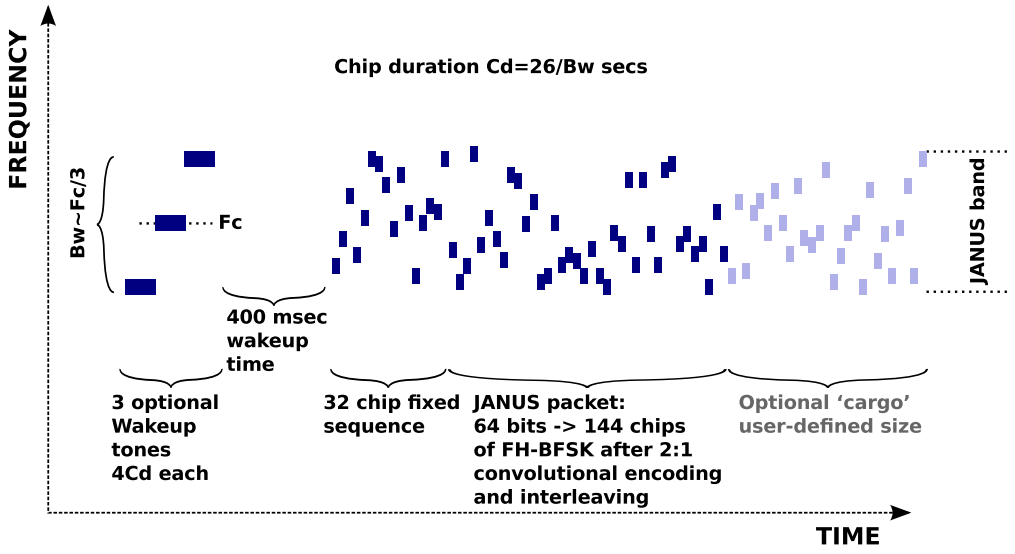


FIGURE 5.6.1: The JANUS signal in a time-frequency plot. From [118]

data block) can be encrypted using conventional techniques to ensure confidentiality, integrity, and authenticity of the exchanged information.

However, given the characteristics of underwater acoustic communications (i.e., limited bandwidth, reduced bit rate, long propagation delay, and possible intermittent connectivity), some traditional cryptography approaches may be less practical and effective in underwater acoustic networks, as discussed in Section 5.4.1.

In the world of consumer terrestrial communications, it is often taken for granted that devices 'just connect' to each other. The Wi-Fi standard [298], for example, is so ubiquitous that it has become synonymous with internet access. This strict standardization extends well below the surface, with applications that are completely unaware of the complexities of the network that exist below them, and even components of the networking stack operating agnostic to each other. This idea of modular and interoperable systems permeates even down to the hardware layer: a PC can access the internet regardless of the brand or model of the networking card currently installed, and this can even be replaced with a USB dongle, and service continues uninterrupted. A quick driver download is often all that is required.

This is a far cry from the world of underwater communications networks. As discussions, in underwater networks, acoustic communications is the predominant modality, with acoustic modems being fitted to surface buoys, bottom buoys, ocean vessels, and remote underwater vehicles [299; 300; 256], to name but a few. Each of these devices will run a manufacturer's proprietary communications protocol. The only option for running a large-scale network is to outfit all the nodes with compatible modems. This rapidly inflates the cost of introducing changes to the modems on a vehicle, since changing the manufacturer will require a complete refitting of the entire fleet to maintain full interoperability. Recent developments in open standard

underwater communications standards have made significant headway in this area; for example, the JANUS protocol [118] (developed by the CMRE) is an open source underwater communication protocol; which is already available from some manufacturers. While there is some adoption, it is far from being a ubiquitous standard.

This lack of flexibility extends into the design of the networking stack. There are ongoing efforts to develop new techniques for underwater communications, some of which have been highlighted in this section, are shown in the literature. These describe novel adaptations to elements of the protocol stack, such as adaptive physical layers or smart networking protocols. To actually implement this requires integration with existing systems, which is a slow and tedious process, often requiring applications to be customized to take advantage of the new communications solution.

Much like any peripheral device, each modem has a unique interface. While similarities do exist between similar product lines, each modem does require an integration activity to enable access from the platform's code base. This makes integration tasks much slower, as the communications stack must be re-written to cope with the specifics of the modem being used. Many systems do not utilise a separate communications stack; instead, they make the communications behaviour a core part of the application. This can make development easier but means that a change in modem hardware requires a rewrite of the application.

All of this contributes to raising the bar of entry needed to develop applications to run on underwater systems. A designer (or their team) must have knowledge of not only the desired system but also of the entire communications stack.

5.6.2 Upgrading JANUS

It is widely recognized that JANUS, the current NATO standard, while an essential initial step to interoperability [2; 118], is not the final stage of this journey, and an evolution of JANUS is required to meet increasingly demanding operational requirements.

Several research papers have presented potential areas where JANUS may wish to be upgraded, importantly including some authored by the original JANUS specification team.

Within [301], Green and Dellamorte proposed that within any list of potential upgrades for JANUS, the following four are important:

1. Compensation for severe frequency offset;
2. Multi-access support and interference reduction;

3. Compensation for range rate (relative speed);
4. Precision ranging while retaining standard noncoherent acquisition robustness.

Equally, within [294], the following are listed as potential upgrades by Alves et al. from the Centre for Maritime Research and Experimentation (CMRE):

1. JANUS fast modes;
2. Additional frequency bands;
3. Security;
4. Standardizing the language switching mechanism;
5. Establishing ID assignment mechanisms;
6. Other applications and populating the User Class and Application Type fields;
7. Going beyond STANAG status.

In order to tackle these concerns, it is proposed to introduce the Phorcys protocol suite to address the following areas raised within [294] and [301]:

1. Communications and Transmission Security;
2. Robust Performance in Challenging channels;
3. Multi-access support and interference reduction (including enhanced networking);
4. High Data Rate modes (flexibility of data rates);
5. Multiple Frequency Bands.

Furthermore, the introduction of Phorcys seeks to embody the ethos as set out by the original authors of JANUS within [118] by fully specifying the signal encoding and message format as well as making freely available a reference transmitter/receiver in MATLAB so that anyone can communicate with Phorcys.

While JANUS was originally conceived to be a deliberately simple protocol to enable easy adoption by legacy equipment, Phorcys instead aims to provide high performance, interoperability, and security by design to meet the demanding needs of underwater users: the scalability to different size, weight, and power devices is given by a multi-band approach sharing common baseband processing.

5.6.3 The House of JANUS

In order to provide an enduring capability evolution of JANUS, the concept of a House of JANUS is proposed. The development of this concept provides a framework for future enhancements to the JANUS standard, such as those offered by the Phorcys communications suite. Every "room" is required to have a robust underwater communications infrastructure.

A visualisation of the concept around the House of JANUS can be observed in figure 5.6.2. The current STANAG 4748 (ANEP-87) is in the bottom-left room of the house.

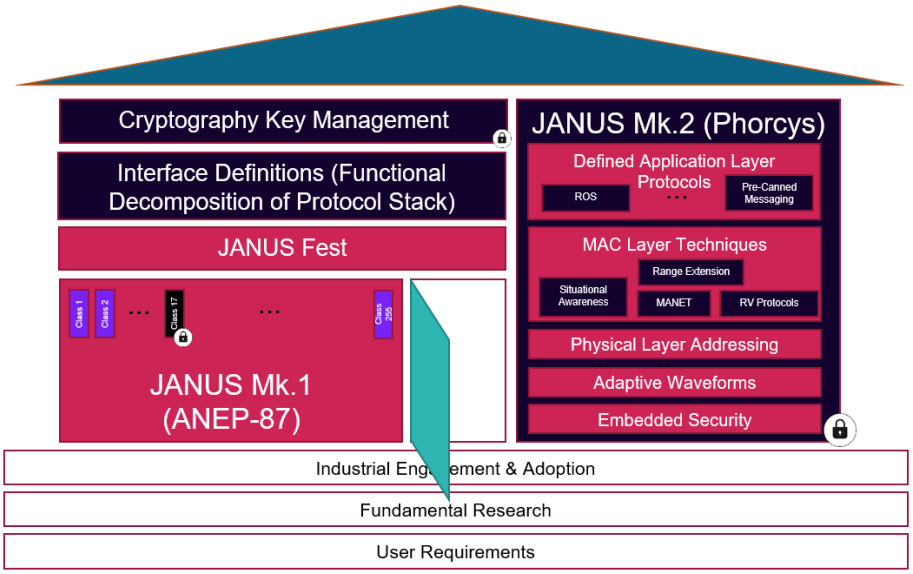


FIGURE 5.6.2: A concept for the House of JANUS

The house itself is built upon a strong foundation of Industrial Engagement and Adoption, Fundamental Research, and User Requirements to ensure that the output provides optimal communication systems to meet extant and emerging needs. Examples of these may include the JANUS fest [302], the UComms series of conferences, NATO research task groups such as NATO IST 174 [2], or NATO Industry Advisory Groups (such as NIAG SG190 and SG243).

On the right side of the house, we can see some aspects presented by the adoption of the Phorcys communications protocol stack, such as security, adaptive waveforms, physical layer addressing, and advanced MAC techniques.

Furthermore, other aspects of the JANUS community may be included within the House of JANUS, such as future interoperability test events, based upon the success of JANUS Fest [302] or the ability to define cross-stack interfaces, such as those proposed in [116].

Within this section, a novel communications protocol suite, known as Phorcys, has been presented as an evolution of the current JANUS specification to meet challenging operational requirements, including security and reliability in a series of differing operational environments. Furthermore, the concept of the House of JANUS is presented as a framework for providing continuing improvement in the field of open, interoperable acoustic communications standards.

The Phorcys waveform multiband/multimode family aligns with future military needs for secure, open, and interoperable subsea command and control with integrated acoustic networking and navigation capabilities. The waveform architecture is extensible and flexible, and aligned with hardware-agnostic, software-defined modem open architecture design principles, underpinned by documented specifications for waveform, media layer architecture, and security. It is this open architecture that enables future interoperability.

Within the JANUS standards group, which is responsible for the development of STANAG 4784, known as the JANUS support team, the Phorcys communications specifications have been shared along with the concept for the house of JANUS, and it is hoped they will lead to a collective step change in the way NATO does underwater communications standardisation, thus enabling resilient communications for tactical systems.

5.7 Chapter Conclusion

In this chapter, a holistic approach to developing secure and interoperable communications systems to meet the challenging needs of NATO has been introduced; it has been demonstrated how this approach enables security to be met with no overhead in the protocol itself. Performance trials of the protocols are further demonstrated in papers published by co-authors in [7; 6] but are not presented in this thesis.

Within the chapter, the motivations were presented to develop a novel communications protocol stack, and the use cases which need to be met were articulated, including some motivating reasons for reduction of power usage. The channel environment relating to underwater acoustics was also briefly discussed to motivate some physical layer design approaches, these channels were directly relevant to the use cases presented in Section 5.1.

Following these motivations, a novel approach to physical layer design with embedded security was introduced, including how this approach meets the needs of the aforementioned use cases, as well as a discussion on approaches to enable said security,

in turn it was discussed how this would be enabled and supported by the emerging capability of autonomous vehicles.

Finally, within the chapter, we are presented on approaches that can be taken as the next steps to enable standardisation and ensure interoperability across NATO, creating operational capability from the work presented in this Thesis.

It is within this context of standardisation that the techniques proposed within this chapter offer the most benefit, as the current standard, JANUS [118; 245], does not meet the operational requirements as articulated within this chapter. In particular, JANUS does not include any security or efficiency approaches and as is designed as a minimal standard for interoperability. The techniques proposed in this chapter, specifically around Phorcys will meet these needs with 256-bit AES security integrated into the communications stack with a high performance and flexible physical layer to enable the needs of the use cases to be met if standardised.

This chapter has covered a breadth of the thesis including, (briefly) source coding, channel coding, modulation and the channel itself. It also provides the closing chapter to the technical aspects of the thesis before the thesis concludes in Chapter 6.

Chapter 6 : Discussion and Conclusions

This chapter serves as the concluding remarks for the thesis, providing a comprehensive overview of key topics explored within the context of resilient communications for tactical communication. Throughout the thesis, various aspects of resilient communication strategies in tactical scenarios have been discussed and analysed.

The positioning of Chapter 6 can be seen within the structure of the overall thesis in figure 6.1.1.

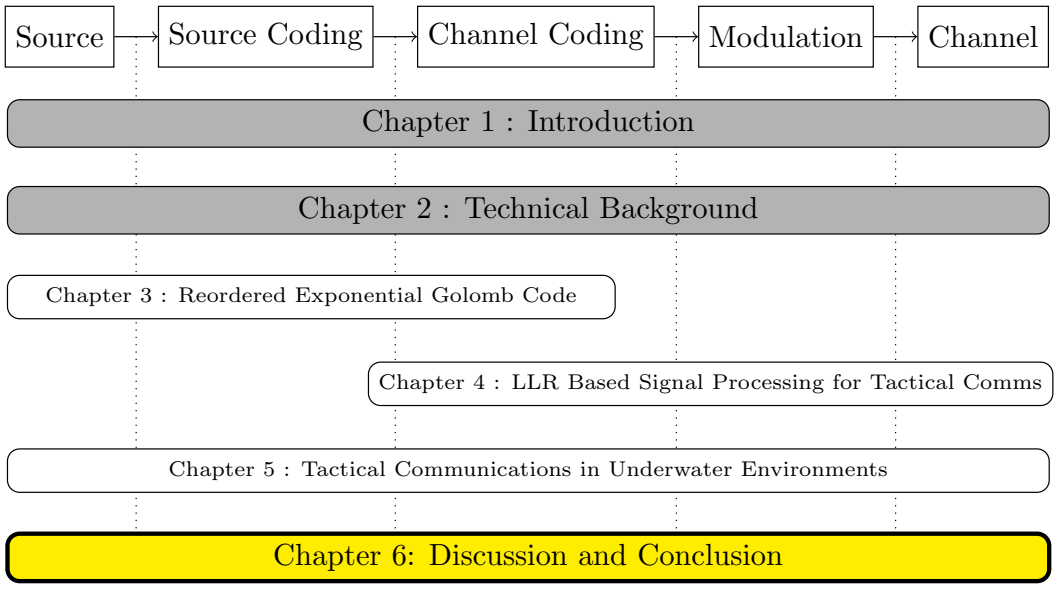


FIGURE 6.1.1: Structure of the Thesis

6.1 Conclusions

As can be seen in figure 6.1.1, this chapter offers a 'bookend' to the thesis itself and will cover all areas from source to channel as we conclude all the individual chapters.

During this thesis, various aspects of communications system design have been explored in depth to understand their overall performance, these specific novel contributions have been demonstrated to improve the performance of wireless communications in challenging communications environment. Specifically, a number of these have been published within the body of scientific work in [1; 2; 3; 4; 5; 6; 7; 8], these publications are peer-reviewed contributions demonstrating the efficacy of the work done within this thesis. As well as these peer-reviewed publications, numerous 3GPP standards contributions have been developed (nearly 100), however as these do not directly relate to tactical communications they are not included within this thesis.

Within **Chapter 1**, an overview of the thesis was presented, along with some motivations and some initial discussions of the work presented in the thesis.

This was followed by **Chapter 2** which provides the reader with some technical background on various wireless communications and information theory topics that are pertinent to the thesis and enables the technical discussion on the benefits and methodology in further chapters to enable resilient communications for tactical systems. Specifically , within this chapter the reader is introduced to information sources, source coding, channel coding, channel capacity, modulation, security, entropy, mutual information and standards.

The research conducted has yielded substantial contributions to the field of wireless communications. This is showcased in **Chapter 3** where proof of concept for multiple innovative LLR based signal processing techniques has been established, including a novel approach to enhance the performance and flexibility of M-ary Orthogonal Signalling communications scheme and a novel sub-block turbo equalizer for a CPM modulation scheme, which shows benefits in relevant operational deployments and performance within 1.1 dB of the CCMC bound. Both of these techniques enhance the resilience of tactical communications through the development of LLR-based signal processing techniques.

These contributions are continued in **Chapter 4** where the reader is presented with the overall performance of a pioneering joint source-channel code and communication code, the RExpGEC code along with the novel RExpGEC-URC-QPSK scheme, which shows near-capacity performance for a number of different information sources, remaining within 2.2 dB of the DCMC capacity for any given zeta distributed information source.

Within **Chapter 5** these novel contributions continue with the introduction of the novel Phorcys communication scheme which offers a high performance, flexible and

secure underwater acoustic communications stack to enable high-tempo tactical communications in extremely challenging environments.

Collectively, these chapters present key contributions to the field of wireless communications, notably in increasing the resilience of tactical communications.The efficacy of these contributions is supported by a substantial portfolio of peer-reviewed and published material.

6.2 Advancements in Wireless Communications

The techniques discussed in this thesis mark a significant stride towards achieving near-capacity performance in wireless communication systems. These advancements establish the feasibility of novel techniques and demonstrate their efficacy in enhancing the overall performance of communication systems.

These details of the different novel techniques and how they relate to the specific fields of source coding, channel coding and modulation are discussed further in Sections 6.2.1 to 6.2.3, whereby a more detailed conclusion is discussed for each technology area.

6.2.1 Source Coding

Initially, the Thesis presents an overview of respective prior work in source coding through a survey of source and channel coding published material in Chapter 2.

During Chapter 3, **a novel joint source and channel coding scheme was proposed, the RExpGEC-URC-QPSK** scheme, which can be used in various channels with a different information sources. This has been shown to have information and channel performance efficiency, and provides performance within 2.2 dB of the DCMC capacity, this further demonstrates the ability for this novel RExpGEC code to have optimal performance regardless of source distribution.

The universal information source approach allows for use of the code in many communications link, and the novel scheme is based on the source distribution of the zeta distribution, which is shown to be a common occurring source distribution.

The thesis further explores elements of source coding are implicitly explored in Chapter 5 whereby the Phorcys communications scheme is specifically designed to meet the needs of different encoded source information and source distributions, such as those observed in maritime mine countermeasures or through voice communications.

6.2.2 Channel Coding

In Chapter 2, a survey of state-of-the-art channel coding is briefly explored, and this will be further expanded upon in future iterations of this thesis, with a particular emphasis on short block length coding approaches.

Channel coding is then delved into more deeply in Chapter 3 of the thesis, where the reader is introduced to the novel **RExpGEC-URC-QPSK** scheme. By utilizing a novel trellis encoder and decoder, this scheme offers near-capacity performance and can provide efficient performance across various channel types.

The emphasis on short block lengths is crucial for Underwater Acoustic communications due to the inherently limited bandwidth available. The schemes proposed in Chapter 4, employing **M-ary Orthogonal Signalling** and the **NATO Narrowband waveform**, also have blocks that are typically sub-1000 bits in length. In these cases, correctly scaling the LLRs from a demodulator is essential for achieving good communication performance. Approaches for this, as well as enhanced LLR-based signal processing, are discussed within Chapter 4.

Finally, in Chapter 5, channel coding is further explored, this time incorporating symbol-level Reed Solomon decoding to provide resilience to the tactical communications standard that is **Phorcys**.

6.2.3 Modulation Scheme

In Chapter 4, a modulation scheme as well as a novel method for decoding bit-level LLRs are proposed. These aim to enable flexible and high-performance channel and source coding techniques, as well as improved communications and information security. Two novel schemes for demodulation and modulation are introduced: **one for generating bit level LLRs from M-ary orthogonal signalling**, and another for **Sub Block Turbo Equalizer** of differentially encoded Continuous Phase Modulation (CPM) modulation.

This modulation scheme is suggested for use in a UK underwater communications standard, **Phorcys**, which is introduced in Chapter 5. It will enable new levels of flexibility and security by accommodating variable-length a priori payloads in accordance with new and legacy cryptographic schemas.

6.3 Contributions outside of Thesis

In tandem with the focused contributions to this thesis, substantial efforts have been dedicated by the author to the development of additional components essential for the

eventual deployment of wireless communication capabilities. These efforts extend beyond the immediate scope of this thesis, encompassing a multifaceted approach.

6.3.1 Development of Supporting Facets

Several key facets have undergone significant development to fortify the foundation for the deployment of wireless communication systems. These include the development of several ecosystems and projects, including the CETO underwater communications community, leading the NATO Research Task Group on secure underwater communications, and leading the NATO Wireless Communications Standardisation Project.

6.3.2 Leadership in Standardization

A central pillar of the author's comprehensive initiative is the assumption of a leadership role in standardization processes. By actively participating in and contributing to the formulation of standards within both 3GPP and NATO, we are committed to guaranteeing the interoperability and smooth integration of the envisioned wireless communication systems into the broader industry landscape. This proactive engagement underscores the dedication to ensuring that our proposed systems align seamlessly with established standards, fostering a cohesive and interoperable technological environment.

6.3.3 Industry Adoption Initiatives

The focus has been on streamlining the integration of emerging technologies into the industry. During the author's tenure at Dstl, collaborative initiatives with key industry stakeholders through various contracted activities have played a pivotal role in fostering the adoption of innovative wireless communication techniques. This concerted effort has proven instrumental in bringing novel and fundamental advancements from the research realm into practical implementation within the industry.

6.3.4 UK IEEE Community

In multifaceted roles, such as Chair, Vice-Chair, and Treasurer within the UK IEEE Information Theory community, the author has spearheaded efforts to cultivate a vibrant community dedicated to advancing wireless communication and information theory technology. Through effective leadership, the author has played a pivotal role in steering the community towards the development of innovative technologies, contributing significantly to the evolution of the field.

6.3.5 Future Deployment Prospects

The strategic consolidation of these efforts positions the wireless communication capabilities developed within this thesis for future deployment in deployable communications systems. The groundwork laid in terms of standards, industry acceptance, and ecosystem development establishes a well-prepared platform for a seamless transition from initial research to practical implementation.

While this broader initiative extends beyond the scope of the work detailed in this thesis, it maintains an intrinsic and vital connection. The initiatives undertaken to facilitate deployment align seamlessly with the overarching objective of advancing wireless communication systems, thereby imparting a tangible and practical dimension to the theoretical contributions expounded in this thesis.

6.4 Future Work

The completion of this thesis unveils potential avenues for future research, extending beyond the current endeavours. The following areas present promising directions for further exploration:

- While this thesis marks the introduction of the RExpGEC-URC-QPSK and the RExpGEC schemes, neither has undergone hardware implementation nor inclusion in a communications standard. The practicality of these schemes within a network—addressing aspects like integration with an IP network—merits consideration.
- In the context of the RExpGEC-URC-QPSK, a potential avenue is the development of early stopping criteria within the scheme to enable complexity reduction. This increase in complexity, compared to Separate Source and Channel Coding benchmarks, could potentially be mitigated by such approaches, albeit at the cost of performance. If coupled with a Channel State Information feedback approach incorporating variable Modulation and Coding Schemes, this could provide a robust framework for balancing complexity and performance across a communications link.
- The 'depth' parameter of the RExpGEC could be further developed to comprehend the interplay between complexity and performance. While the RExpGEC inherently offers flexibility, the extent to which this contributes to improved performance is not explicitly quantified.
- The M-ary orthogonal signalling decoder approach introduced in Chapter 3 to facilitate bit-level LLR definition has been assessed in terms of its performance

concerning Mutual Information. However, its evaluation within an overall communications scheme remains unexplored. This could be a prospective avenue of research, explicitly incorporated into the subsequent phases of Phorcys activity, as discussed in Chapter 5.

- The SB-TE presented in Chapter 3 is yet to be implemented in hardware. This implementation could provide insights into the radiated performance of such a system beyond the idealized performance observed in simulations.
- Further analysis of the dominant error mechanisms at high Signal-to-Noise Ratios (SNRs) in the SB-TE is warranted. This analysis could lead to further optimisation of the SB-TE for improved performance.
- The work presented in Chapter 5 signifies an ongoing effort to develop a high-performance communications protocol stack for underwater communications and to establish standards for such an ecosystem. While several practical steps for the Phorcys activity and Venilia have been proposed, a critical step would involve setting up a formal standards structure within NATO. This structure would facilitate the contribution and consensus-driven development of standards that align with NATO's requirements.

In addition to these potential avenues, numerous other directions for future research can be explored based on the findings presented in this thesis.

6.5 Closing Remarks

This thesis has presented several novel techniques to improve the performance of wireless communications in tactical environments. This work has and will continue to be presented to and inform future standards and developments in both NATO and 3GPP.

In conclusion, the efforts undertaken beyond the scope of this thesis underscore a commitment to transforming theoretical advancements into tangible, deployable wireless communication capabilities. The journey from conception to deployment involves a dynamic interplay of standardization, industry engagement, and ecosystem development, each contributing to the realization of a robust and effective wireless communication infrastructure.

Ultimately, the work shown in this thesis does not present the end of the journey but merely the starting point.

References

[1] **Hamilton, Alexander**, S. Holdcroft, D. Fenucci, P. Mitchell, N. Morozs, A. Munafò, and J. Sitbon, "Adaptable Underwater Networks: The Relation between Autonomy and Communications," *Remote Sensing*, vol. 12, no. 20, p. 3290, 2020.

[2] **Hamilton, Alexander**, J. Barnett, A.-M. Hobbs, K. Pelekanakis, R. Petroccia, I. Nissen, and D. Galsdorf, "Towards Secure and Interoperable Underwater Acoustic Communications: Current Activities in NATO IST-174 Research Task Group," *Procedia Computer Science*, vol. 205, pp. 167–178, 2022.

[3] **Hamilton, Alexander**, J. Barnett, and A.-M. Hobbs, "Phorcys, an evolution of JANUS," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022.

[4] **Hamilton, Alexander**, M. El-Hajjar, and R. G. Maunder, "Reordered Exponential Golomb Error Correction Code for Universal Near-Capacity Joint Source-Channel Coding," *IEEE Access*, 2023.

[5] A.-M. Hobbs, J. Barnett, and **Hamilton, Alexander**, "PCIS-A Novel Approach to Security in the UW Domain," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022.

[6] J. Davies, P. Randall, J. Neasham, B. Sherlock, and **Hamilton, Alexander**, "Phorcys Waveform Architecture," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022.

[7] J. Neasham, T. Corner, J. Davies, and **Hamilton, Alexander**, "Sea Trial Results and Receiver Performance Analysis for Phorcys V0 Waveform," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–5, IEEE, 2022.

[8] J. Kellett, **Hamilton, Alexander**, J. Williams, and C. H. Wong, "Sub-Block Turbo Equalization for CPM Waveforms in Multipath Environments," in *2023 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–6, IEEE, 2023.

[9] **Hamilton, Alexander**, "EXIT Chart Analysis of the UMTS Turbo Code in VLF Channels," in *International Zurich Seminar on Communications-Proceedings*, ETH-Zürich, 2016.

[10] **Hamilton, Alexander**, P. Agard, F. Paris, B. Bertenyi, K. Spruyt, K. Murphy, and D. Peterson, "Standards-Based Agile Radio Systems and Tactical Interoperability; the use of 3GPP protocols in tactical networks," tech. rep., EasyChair, 2023.

[11] **Hamilton, Alexander**, "R4-2300056 4Tx BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 02 2023.

[12] **Hamilton, Alexander**, "R4-2300057 Effect of multiple uplink repetitions on UE demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 02 2023.

[13] **Hamilton, Alexander**, "R4-2300058 Effect of multiple uplink repetitions on SAN demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 02 2023.

[14] **Hamilton, Alexander**, "R4-2304048 Supporting results for 4Tx Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 03 2023.

[15] **Hamilton, Alexander**, "R4-2304045 TP for 38.181 Introduction of SAN demodulation requirements for IoT-NTN," tech. rep., Nokia, Nokia Shanghai Bell, 03 2023.

[16] **Hamilton, Alexander**, "R4-2304046 Comment on UL Pre-Compensation Gap and Number of Segments," tech. rep., Nokia, Nokia Shanghai Bell, 03 2023.

[17] **Hamilton, Alexander**, "R4-2304047 Discussion on 4Tx BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 03 2023.

[18] **Hamilton, Alexander**, "R4-2307021 pCR for introduction of SAN Demodulation requirements," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[19] **Hamilton, Alexander**, "R4-2307022 Discussion on SAN demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[20] **Hamilton, Alexander**, "R4-2307023 General Discussion on 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[21] **Hamilton, Alexander**, "R4-2307024 Discussion on PDSCH Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[22] **Hamilton, Alexander**, "R4-2307025 Supporting Simulation results for PDSCH demod for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[23] **Hamilton, Alexander**, "R4-2307026 Discussion on SDR Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[24] **Hamilton, Alexander**, "R4-2307027 Supporting Simulation results for SDR demod for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[25] **Hamilton, Alexander**, "R4-2307028 Discussion on CQI Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[26] **Hamilton, Alexander**, "R4-2307029 Supporting Simulation results for CQI demod for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[27] **Hamilton, Alexander**, "R4-2307030 Discussion of 4Tx Demodulation Requirements," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[28] **Hamilton, Alexander**, "R4-2307031 Supporting simulations for 4Tx Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[29] **Hamilton, Alexander**, "R4-2307032 draftCR for 38.104 - inclusion of 4Tx Requirements," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[30] **Hamilton, Alexander**, "R4-2307033 Discussion on UE Demodulation for non-collocated FR1 intra-band EN-DC/NR-CA," tech. rep., Nokia, Nokia Shanghai Bell, 05 2023.

[31] **Hamilton, Alexander**, "R4-2311070 CR on TS 36.181 for SAN Demodulation on PUSCH," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[32] **Hamilton, Alexander**, "R4-2311071 General Discussion on 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[33] **Hamilton, Alexander**, "R4-2311072 Discussion on PDSCH Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[34] **Hamilton, Alexander**, "R4-2311073 Supporting Simulation results for PDSCH demod for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[35] **Hamilton, Alexander**, "R4-2311074 Discussion on SDR Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[36] **Hamilton, Alexander**, "R4-2311075 Supporting Simulation results for SDR demod for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[37] **Hamilton, Alexander**, "R4-2311076 Discussion on CQI Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[38] **Hamilton, Alexander**, "R4-2311077 Supporting Simulation results for CQI demodulation for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[39] **Hamilton, Alexander**, "R4-2311078 draftCR for 38.101 - inclusion of 8Rx Applicabilty Rule," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[40] **Hamilton, Alexander**, "R4-2311079 Discussion of 4Tx Demodulation Requirements," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[41] **Hamilton, Alexander**, "R4-2311080 Supporting simulations for 4Tx Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[42] **Hamilton, Alexander**, "R4-2311081 draftCR for 38.104 - inclusion of 4Tx Requirements," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[43] **Hamilton, Alexander**, "R4-2311082 Discussion on UL 256 QAM BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[44] **Hamilton, Alexander**, "R4-2311083 Supporting simulations for UL 256 QAM BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[45] **Hamilton, Alexander**, "R4-2313941 CR on TS 36.181 for SAN Demodulation on PUSCH," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[46] **Hamilton, Alexander**, "R4-2313879 draftCR for 38.101 - inclusion of 8Rx Applicabilty Rule," tech. rep., Nokia, Nokia Shanghai Bell, 08 2023.

[47] **Hamilton, Alexander**, "R4-2314257 Topic summary for NR RF FR2 req Ph3 Demod (256 QAM BS Demod)," tech. rep., Moderator (Nokia), 08 2023.

[48] **Hamilton, Alexander**, "R4-2313946 WF for NR RF FR2 req Ph3 Demod (256 QAM BS Demod)," tech. rep., Moderator (Nokia), 08 2023.

[49] **Hamilton, Alexander**, "R4-2316903 WF on 256QAM BS demodulation," tech. rep., Nokia, 10 2023.

[50] **Hamilton, Alexander**, "R4-2316972 Simulation summary for 256QAM," tech. rep., Nokia, 10 2023.

[51] **Hamilton, Alexander**, "R4-2315032 Discussion on BS Demodulation on Less than 5 MHz," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[52] **Hamilton, Alexander**, "R4-2315033 Supporting Simulations for BS Demodulation on Less than 5 MHz," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[53] **Hamilton, Alexander**, "R4-2315034 Discussion on 8Rx general demodulation aspects," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[54] **Hamilton, Alexander**, "R4-2315035 Discussion on PDSCH Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[55] **Hamilton, Alexander**, "R4-2315036 Supporting Simulation results for PDSCH demodulation for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[56] **Hamilton, Alexander**, "R4-2315037 Discussion on SDR Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[57] **Hamilton, Alexander**, "R4-2315038 Supporting Simulation results for SDR demodulation for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[58] **Hamilton, Alexander**, "R4-2315039 Discussion on CQI Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[59] **Hamilton, Alexander**, "R4-2315040 Supporting Simulation results for CQI demodulation for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[60] **Hamilton, Alexander**, "R4-2315041 Introduction of 8Rx Applicability Rule," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[61] **Hamilton, Alexander**, "R4-2315042 Supporting simulations for 4Tx Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[62] **Hamilton, Alexander**, "R4-2315043 Introduction of 4Tx PUSCH requirements," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[63] **Hamilton, Alexander**, "R4-2315044 Discussion on UL 256 QAM BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[64] **Hamilton, Alexander**, "R4-2315045 Supporting Simulations for 256QAM UL Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[65] **Hamilton, Alexander**, "R4-2315046 Discussion on MIMO evolution BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[66] **Hamilton, Alexander**, "R4-2315047 Simulations for MIMO evolution BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[67] **Hamilton, Alexander**, "R4-2315048 Discussion on Coverage Enhancement BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[68] **Hamilton, Alexander**, "R4-2315049 Simulations for Coverage Enhancement BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[69] **Hamilton, Alexander**, "R4-2315050 Discussion on NR NTN SAN Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[70] **Hamilton, Alexander**, "R4-2315051 NR NTN UE demodulation disussion," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[71] **Hamilton, Alexander**, "R4-2315052 LS Reply on IoT NTN," tech. rep., Nokia, Nokia Shanghai Bell, 10 2023.

[72] **Hamilton, Alexander**, "R4-2318041 Discussion on BS Demodulation on Less than 5 MHz," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[73] **Hamilton, Alexander**, "R4-2318042 Supporting Simulations for BS Demodulation on Less than 5 MHz," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[74] **Hamilton, Alexander**, "R4-2318043 Discussion on 8Rx general demodulation aspects," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[75] **Hamilton, Alexander**, "R4-2318044 Discussion on PDSCH Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[76] **Hamilton, Alexander**, "R4-2318045 Supporting Simulation results for PDSCH demodulation for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[77] **Hamilton, Alexander**, "R4-2318046 Discussion on SDR Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[78] **Hamilton, Alexander**, "R4-2318047 Discussion on CQI Demodulation Requirements for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[79] **Hamilton, Alexander**, "R4-2318048 Supporting Simulation results for CQI demodulation for 8Rx," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[80] **Hamilton, Alexander**, "R4-2318049 Introduction of 8Rx Applicability Rule," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[81] **Hamilton, Alexander**, "R4-2318050 Introduction of 8Rx CA Performance Requirements," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[82] **Hamilton, Alexander**, "R4-2318051 Disucssion on 4Tx Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[83] **Hamilton, Alexander**, "R4-2318052 Discussion on UL 256 QAM BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[84] **Hamilton, Alexander**, "R4-2318053 Supporting Simulations for 256QAM UL Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[85] **Hamilton, Alexander**, "R4-2318054 Discussion on MIMO evolution BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[86] **Hamilton, Alexander**, "R4-2318055 Simulations for MIMO evolution BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[87] **Hamilton, Alexander**, "R4-2318056 Discussion on Coverage Enhancement BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[88] **Hamilton, Alexander**, "R4-2318057 Simulations for Coverage Enhancement BS Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[89] **Hamilton, Alexander**, "R4-2318058 Discussion on NR NTN SAN Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[90] **Hamilton, Alexander**, "R4-2318059 NR NTN UE demodulation discussion," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[91] **Hamilton, Alexander**, "R4-2318060 CR on TS 36.181 for SAN Demodulation," tech. rep., Nokia, Nokia Shanghai Bell, 11 2023.

[92] A. Pérez-Pascual, **Hamilton, Alexander**, R. G. Maunder, and L. Hanzo, "Conceiving Extrinsic Information Transfer Charts for Stochastic Low-Density Parity-Check Decoders," *IEEE Access*, vol. 6, pp. 55741–55753, 2018.

[93] M. Zheng, **Hamilton, Alexander**, and C. Ling, "Covert Communications with a Full-Duplex Receiver in Non-Coherent Rayleigh Fading," *IEEE Transactions on Communications*, 2020.

[94] Y. Livran, V. Le Nir, S. Couturier, M. Suchanski, P. Kaniewski, J. Romanik, **Hamilton, Alexander**, P. Howland, and M. D. Tracy, "Electromagnetic environment situational awareness," in *2021 International Conference on Military Communication and Information Systems (ICMCIS)*, pp. 1–8, IEEE, 2021.

[95] E. Guler, C. Geldard, **Hamilton, Alexander**, and W. Popoola, "Subcarrier intensity modulation for turbulent underwater optical wireless communications," in *2021 Conference on Lasers and Electro-Optics (CLEO)*, pp. 1–2, IEEE, 2021.

[96] W. O. Popoola, C. Geldard, E. Guler, and **Hamilton, Alexander**, "Underwater optical wireless communication with subcarrier intensity modulation: an experimental demonstration," in *Proceedings of Meetings on Acoustics*, vol. 44, AIP Publishing, 2021.

[97] N. Morozs, P. Mitchell, D. Grace, T. Tozer, T. Bauge, and **Hamilton, Alexander**, "Phorcys Networking," *UCOMMS-22*, 2022.

[98] C. T. Geldard, E. Guler, **Hamilton, Alexander**, and W. O. Popoola, "An empirical comparison of modulation schemes in turbulent underwater optical wireless communications," *Journal of Lightwave Technology*, vol. 40, no. 7, pp. 2000–2007, 2022.

[99] J. Chen, C. T. Geldard, E. Guler, **Hamilton, Alexander**, and W. O. Popoola, "An Experimental Demonstration of FSK-SIM-PDM Underwater Optical Wireless Communications," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022.

[100] C. T. Geldard, E. Guler, I. M. Butler, **Hamilton, Alexander**, and W. O. Popoola, "Exploiting polarisation state for beyond 10 Gbps underwater optical wireless data transmission in hostile channel conditions," in *Next-Generation Optical Communication: Components, Sub-Systems, and Systems XII*, vol. 12429, pp. 172–175, SPIE, 2023.

[101] N. A. G. O. EMERGING and D. TECHNOLOGIES, *Annual Report 2021*. NATO, 2021.

[102] H. Treasury, *Spending review 2020*. HM Government, 2020.

[103] S. Ten Brink, "Convergence of iterative decoding," *Electronics letters*, vol. 35, no. 10, pp. 806–808, 1999.

[104] N. S. OFFICE, "Narrowband Waveform for VHF/UHF Radio - Physical Layer Standard and Propagation Models," STANAG 5631/AComP-5631 (Draft), NATO, Dec 2016.

[105] S. Ten Brink, J. Speidel, and R.-H. Yan, "Iterative demapping for QPSK modulation," *Electronics letters*, vol. 34, no. 15, pp. 1459–1460, 1998.

[106] T. Wang, M. F. Brejza, W. Zhang, R. G. Maunder, and L. Hanzo, "Reordered Elias Gamma error correction codes for the near-capacity transmission of multimedia information," *IEEE Access*, vol. 4, pp. 5948–5970, 2016.

[107] S. Golomb, "Run-length encodings (Corresp.)," *IEEE transactions on information theory*, vol. 12, no. 3, pp. 399–401, 1966.

[108] S. Mui, "Convolutional code performance in the rician fading channel," *IEEE Transactions on Communications*, vol. 24, no. 6, pp. 592–606, 1976.

[109] **Hamilton, Alexander**, J. Davies, and J. Neasham, "PhorcysV0 preliminary waveform specification (PWFSv0)," *WFS/20/007*, 2020.

[110] H. S. Wang and P.-C. Chang, "On verifying the first-order markovian assumption for a rayleigh fading channel model," *IEEE Transactions on Vehicular Technology*, vol. 45, no. 2, pp. 353–357, 1996.

[111] V. Le Nir and B. Scheers, "Low complexity generic receiver for the NATO Narrow Band Waveform," in *2017 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–7, IEEE, 2017.

[112] C. Brown and P. J. Vigneron, "Spectrally Efficient CPM Waveforms for Narrowband Tactical Communications in Frequency Hopped Networks," in *MILCOM 2006 - 2006 IEEE Military Communications conference*, pp. 1–6, Oct 2006.

[113] B. Sherlock, C. C. Tsimenidis, and J. A. Neasham, "Signal and receiver design for low-power acoustic communications using m-ary orthogonal code keying," in *IEEE OCEANS 2015*, 2015.

[114] B. Sherlock, J. A. Neasham, and C. C. Tsimenidis, "Spread-Spectrum Techniques for Bio-Friendly Underwater Acoustic Communications," *IEEE Access*, vol. 6, pp. 4506–4520, 2018.

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

[116] R. Petroccia, G. Zappa, T. Furfaro, J. Alves, and L. D'Amaro, "Development of a Software-Defined and Cognitive Communications Architecture at CMRE," in *OCEANS 2018 MTS/IEEE Charleston*, pp. 1–10, Oct 2018.

[117] K. Pelekanakis, S. A. Yildirim, G. Sklivanitis, R. Petroccia, J. Alves, and D. Pados, "Physical Layer Security against an Informed Eavesdropper in Underwater Acoustic Channels: Feature Extraction and Quantization," in *Proceedings of the 5th IEEE OES International Conference on Underwater Communications and Networking*, UComms20, pp. 1–5, 2021.

[118] J. Potter, J. Alves, D. Green, G. Zappa, I. Nissen, and K. McCoy, "The JANUS underwater communications standard," in *2014 Underwater Communications and Networking (UComms)*, pp. 1–4, IEEE, 2014.

[119] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 623–656, 1948.

[120] E. Lehman and A. Shelat, "Approximation algorithms for grammar-based compression," in *Proceedings of the thirteenth annual ACM-SIAM symposium on Discrete algorithms*, pp. 205–212, Society for Industrial and Applied Mathematics, 2002.

[121] M. V. Mahoney, "Fast Text Compression with Neural Networks.," in *FLAIRS Conference*, pp. 230–234, 2000.

[122] J. Ziv and A. Lempel, "Compression of individual sequences via variable-rate coding," *IEEE transactions on Information Theory*, vol. 24, no. 5, pp. 530–536, 1978.

[123] P. Elias, "Coding for noisy channels," in *IRE International Convention Record*, pp. 37–46, 1955.

[124] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *Proceedings of*

ICC'93-IEEE International Conference on Communications, vol. 2, pp. 1064–1070, IEEE, 1993.

[125] R. Gallager, "Low-density parity-check codes," *IRE Transactions on information theory*, vol. 8, no. 1, pp. 21–28, 1962.

[126] L. Hanzo, R. G. Maunder, J. Wang, and L.-L. Yang, *Near-capacity variable-length coding: regular and EXIT-chart-aided irregular designs*, vol. 20. John Wiley & Sons, 2010.

[127] S. B. Wicker and V. K. Bhargava, *Reed-Solomon codes and their applications*. John Wiley & Sons, 1999.

[128] S. Kallel and D. Haccoun, "Generalized type II hybrid ARQ scheme using punctured convolutional coding," *IEEE transactions on communications*, vol. 38, no. 11, pp. 1938–1946, 1990.

[129] J. Heller and I. Jacobs, "Viterbi decoding for satellite and space communication," *IEEE Transactions on Communication Technology*, vol. 19, no. 5, pp. 835–848, 1971.

[130] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the society for industrial and applied mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[131] R. M. Fano, *The transmission of information*, vol. 65. Massachusetts Institute of Technology, Research Laboratory of Electronics ..., 1949.

[132] C. E. Shannon, "Prediction and entropy of printed English," *Bell system technical journal*, vol. 30, no. 1, pp. 50–64, 1951.

[133] B. Sklar *et al.*, *Digital communications*, vol. 2. Pearson, 2001.

[134] J. G. Proakis and M. Salehi, *Digital communications*, vol. 4. McGraw-hill New York, 2001.

[135] V. G. Cerf, "Ascii format for network interchange," tech. rep., IEEE, 1969.

[136] W. Kinsner and R. Greenfield, "The Lempel-Ziv-Welch (LZW) data compression algorithm for packet radio," in *WESCANEX'91'IEEE Western Canada Conference on Computer, Power and Communications Systems in a Rural Environment'*, pp. 225–229, IEEE, 1991.

[137] D. Grois, T. Nguyen, and D. Marpe, "Coding efficiency comparison of av1/vp9, h. 265/mpeg-hevc, and h. 264/mpeg-avc encoders," in *2016 Picture Coding Symposium (PCS)*, pp. 1–5, IEEE, 2016.

[138] L. Tolstoy, "War and Peace," 1869.

[139] M. W. Marcellin, M. J. Gormish, A. Bilgin, and M. P. Boliek, "An overview of jpeg-2000," in *Proceedings DCC 2000. Data Compression Conference*, pp. 523–541, IEEE, 2000.

[140] M. F. Brejza, L. Li, R. G. Maunder, B. M. Al-Hashimi, C. Berrou, and L. Hanzo, "20 years of turbo coding and energy-aware design guidelines for energy-constrained wireless applications," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 8–28, 2015.

[141] G. D. Lin and C.-Y. Hu, "The riemann zeta distribution," *Bernoulli*, pp. 817–828, 2001.

[142] M. F. Brejza, T. Wang, W. Zhang, D. Al-Khalili, R. G. Maunder, B. M. Al-Hashimi, and L. Hanzo, "Exponential Golomb and rice error correction codes for generalized near-capacity joint source and channel coding," *IEEE Access*, vol. 4, pp. 7154–7175, 2016.

[143] A. N. Philippou, C. Georghiou, and G. N. Philippou, "A generalized geometric distribution and some of its properties," *Statistics & Probability Letters*, vol. 1, no. 4, pp. 171–175, 1983.

[144] D. A. Huffman, "A method for the construction of minimum-redundancy codes," *Proceedings of the IRE*, vol. 40, no. 9, pp. 1098–1101, 1952.

[145] W. C. Lee, "The advantages of using repetition code in mobile radio communications," in *36th IEEE vehicular Technology conference*, vol. 36, pp. 157–161, IEEE, 1986.

[146] D. J. MacKay, *Information theory, inference and learning algorithms*. Cambridge university press, 2003.

[147] R. W. Hamming, "Error detecting and error correcting codes," *The Bell system technical journal*, vol. 29, no. 2, pp. 147–160, 1950.

[148] 3GPP, "TR 21.916, Release description; release 16," tech. rep., 3GPP, Sep 2020.

[149] R. G. Maunder and L. Hanzo, "Iterative decoding convergence and termination of serially concatenated codes," *IEEE transactions on vehicular technology*, vol. 59, no. 1, pp. 216–224, 2009.

[150] F. Alexa, V. Gui, C. Caleanu, and C. Botoca, "Lossless data compression using neural networks," in *WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering*, World Scientific and Engineering Academy and Society, 2008.

[151] J. Schmidhuber and S. Heil, "Sequential neural text compression," *IEEE Transactions on Neural Networks*, vol. 7, no. 1, pp. 142–146, 1996.

[152] Cyan4973, *LZ v1.9.4*, (accessed January, 2024). https://github.com/lz4/lz4/releases/tag/v1.9.4.

[153] Cyan4973, *Zstandard v1.5.5*, (accessed January, 2024). http://facebook.github.io/zstd/.

[154] G. Roelofs and M. Adler, *zlib 1.3*, (accessed January, 2024). https://www.zlib.net.

[155] C. Tharini and P. V. Ranjan, "Design of modified adaptive Huffman data compression algorithm for wireless sensor network," *Journal of Computer Science*, vol. 5, no. 6, p. 466, 2009.

[156] J. Cleary and I. Witten, "Data compression using adaptive coding and partial string matching," *IEEE transactions on Communications*, vol. 32, no. 4, pp. 396–402, 1984.

[157] M. Mahoney, "Data compression programs," 2009.

[158] N. S. OFFICE, "INTEROPERABLE DATA LINKS FOR IMAGING SYSTEMS," STANAG 7085, NATO, Oct 2017.

[159] N. S. OFFICE, "Single and Multichannel VLF and LF on-line broadcast and off-line OOK systems," STANAG 5030/AComP-4724, NATO, Jan 2015.

[160] C. Deng, X. Fang, X. Han, X. Wang, L. Yan, R. He, Y. Long, and Y. Guo, "IEEE 802.11 be Wi-Fi 7: New challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2136–2166, 2020.

[161] Z. G. Ruthberg and R. G. McKenzie, "Audit and Evaluation of Computer Security," *Special Publication (NIST SP) - 500-19*, 1977.

[162] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review," *MIS quarterly*, pp. 989–1015, 2011.

[163] S. Samonas and D. Coss, "The CIA strikes back: Redefining confidentiality, integrity and availability in security.," *Journal of Information System Security*, vol. 10, no. 3, 2014.

[164] S. Deepika and P. Pandiaraja, "Ensuring CIA triad for user data using collaborative filtering mechanism," in *2013 international conference on information communication and embedded systems (ICICES)*, pp. 925–928, IEEE, 2013.

[165] F. Cohen, "A cryptographic checksum for integrity protection," *Computers & Security*, vol. 6, no. 6, pp. 505–510, 1987.

[166] S. Subramanya and B. K. Yi, "Digital signatures," *IEEE Potentials*, vol. 25, no. 2, pp. 5–8, 2006.

[167] W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, and F. Qian, "Secure control of multiagent systems against malicious attacks: A brief survey," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3595–3608, 2021.

[168] F. Piedad and M. Hawkins, *High availability: design, techniques, and processes*. Prentice Hall Professional, 2001.

[169] A. McCullagh and W. Caelli, "Non-repudiation in the digital environment," *First Monday, volume 5, number 8 (August 2000)*, 2000.

[170] R. C. Merkle, "A certified digital signature," in *Conference on the Theory and Application of Cryptology*, pp. 218–238, Springer, 1989.

[171] M. Boreale, R. De Nicola, and R. Pugliese, "Proof techniques for cryptographic processes," *SIAM Journal on Computing*, vol. 31, no. 3, pp. 947–986, 2001.

[172] R. Sandhu and P. Samarati, "Authentication, access control, and audit," *ACM Computing Surveys (CSUR)*, vol. 28, no. 1, pp. 241–243, 1996.

[173] A. Ashikhmin, G. Kramer, and S. ten Brink, "Code rate and the area under extrinsic information transfer curves," in *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, p. 115, IEEE, 2002.

[174] J. Hagenauer, "The EXIT chart-introduction to extrinsic information transfer in iterative processing," in *Signal Processing Conference, 2004 12th European*, pp. 1541–1548, IEEE, 2004.

[175] R. Hudleston, "The Coast Signal Stations and the Semaphore Telegraph," *Royal United Services Institution. Journal*, vol. 55, no. 405, pp. 1450–1454, 1911.

[176] K. A. Kitchen, "Proverbs and wisdom books of the ancient Near East: the factual history of a literary form," *Tyndale Bulletin*, vol. 28, no. 69, p. 114, 1977.

[177] J. Wang, C. Jiang, Z. Han, Y. Ren, and L. Hanzo, "Internet of vehicles: Sensing-aided transportation information collection and diffusion," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 3813–3825, 2018.

[178] O. Languages, *Oxford Dictionary of English*. Oxford University Press, 2020.

[179] P. Elias, "Universal codeword sets and representations of the integers," *IEEE transactions on information theory*, vol. 21, no. 2, pp. 194–203, 1975.

[180] J. B. Connell, "A huffman-shannon-fano code," *Proceedings of the IEEE*, vol. 61, no. 7, pp. 1046–1047, 1973.

[181] M. Wien, "High efficiency video coding," *Coding Tools and specification*, vol. 24, 2015.

[182] J. Teuhola, "A compression method for clustered bit-vectors," *Information processing letters*, vol. 7, no. 6, pp. 308–311, 1978.

[183] S. Even and M. Rodeh, "Economical encoding of commas between strings," *Communications of the ACM*, vol. 21, no. 4, pp. 315–317, 1978.

[184] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[185] B. Krause, L. Lu, I. Murray, and S. Renals, "Multiplicative LSTM for sequence modelling," *arXiv preprint arXiv:1609.07959*, 2016.

[186] S. Kodituwakku and U. Amarasinghe, "Comparison of lossless data compression algorithms for text data," *Indian journal of computer science and engineering*, vol. 1, no. 4, pp. 416–425, 2010.

[187] J. Rissanen and G. Langdon, "Universal modeling and coding," *IEEE Transactions on Information Theory*, vol. 27, no. 1, pp. 12–23, 1981.

[188] A. S. Fraenkel and S. T. Kleinb, "Robust universal complete codes for transmission and compression," *Discrete Applied Mathematics*, vol. 64, no. 1, pp. 31–55, 1996.

[189] D. Salomon, *Data compression: the complete reference*. Springer Science & Business Media, 2004.

[190] J. L. Massey, "Joint source and channel coding," tech. rep., MASSACHUSETTS INST OF TECH CAMBRIDGE ELECTRONIC SYSTEMS LAB, 1977.

[191] J. Rissanen and G. G. Langdon, "Arithmetic coding," *IBM Journal of research and development*, vol. 23, no. 2, pp. 149–162, 1979.

[192] Q. Stout, "Improved prefix encodings of the natural numbers (Corresp.)," *IEEE Transactions on Information Theory*, vol. 26, no. 5, pp. 607–609, 1980.

[193] M. Bernard and B. D. Sharma, "Some combinatorial results on variable length error correcting codes," *Ars Combinatoria*, vol. 25, pp. 181–194, 1988.

[194] R. Bauer and J. Hagenauer, "Symbol-by-symbol MAP decoding of variable length codes," *ITG FACHBERICHT*, pp. 111–116, 2000.

[195] N. Gortz, "Iterative source-channel decoding using soft-in/soft-out decoders," in *2000 IEEE International Symposium on Information Theory*, p. 173, IEEE, 2000.

[196] N. Gortz, "On the iterative approximation of optimal joint source-channel decoding," *IEEE Journal on Selected Areas in Communications*, vol. 19, no. 9, pp. 1662–1670, 2001.

[197] R. G. Maunder, W. Zhang, T. Wang, and L. Hanzo, "A unary error correction code for the near-capacity joint source and channel coding of symbol values from an infinite set," *IEEE Transactions on Communications*, vol. 61, no. 5, pp. 1977–1987, 2013.

[198] T. Wang, W. Zhang, R. G. Maunder, and L. Hanzo, "Near-capacity joint source and channel coding of symbol values from an infinite source set using Elias gamma error correction codes," *IEEE transactions on communications*, vol. 62, no. 1, pp. 280–292, 2013.

[199] T. Wang, *Elias Gamma Error Correction Code*. PhD thesis, University of Southampton, 2016.

[200] N. L. Johnson, A. W. Kemp, and S. Kotz, *Univariate discrete distributions*, vol. 444. John Wiley & Sons, 2005.

[201] G. J. Sullivan, J.-R. Ohm, W.-J. Han, and T. Wiegand, "Overview of the high efficiency video coding (HEVC) standard," *IEEE Transactions on circuits and systems for video technology*, vol. 22, no. 12, pp. 1649–1668, 2012.

[202] A. Haghighi and L. Vanderwende, "Exploring content models for multi-document summarization," in *Proceedings of human language technologies: The 2009 annual conference of the North American Chapter of the Association for Computational Linguistics*, pp. 362–370, 2009.

[203] J. R. Price and M. Rabbani, "Biased reconstruction for JPEG decoding," *IEEE Signal Processing Letters*, vol. 6, no. 12, pp. 297–299, 1999.

[204] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: model and erasure channel properties," *IEEE Transactions on Information Theory*, vol. 50, no. 11, pp. 2657–2673, 2004.

[205] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate (corresp.)," *IEEE Transactions on information theory*, vol. 20, no. 2, pp. 284–287, 1974.

[206] S. Shao, P. Hailes, T.-Y. Wang, J.-Y. Wu, R. G. Maunder, B. M. Al-Hashimi, and L. Hanzo, "Survey of turbo, LDPC, and polar decoder ASIC implementations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2309–2333, 2019.

[207] J. P. Woodard and L. Hanzo, "Comparative study of turbo decoding techniques: An overview," *IEEE Transactions on vehicular technology*, vol. 49, no. 6, pp. 2208–2233, 2000.

[208] D. Divsalar, S. Dolinar, and F. Pollara, "Serial concatenated trellis coded modulation with rate-1 inner code," in *Globecom'00-IEEE. Global*

Telecommunications Conference. Conference Record (Cat. No. 00CH37137), vol. 2, pp. 777–782, IEEE, 2000.

[209] W. Zhang, M. F. Brejza, T. Wang, R. G. Maunder, and L. Hanzo, "Irregular trellis for the near-capacity unary error correction coding of symbol values from an infinite set," *IEEE Transactions on Communications*, vol. 63, no. 12, pp. 5073–5088, 2015.

[210] Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, D. Chandra, S. X. Ng, and L. Hanzo, "Serially concatenated unity-rate codes improve quantum codes without coding-rate reduction," *IEEE Communications Letters*, vol. 20, no. 10, pp. 1916–1919, 2016.

[211] Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, D. Chandra, S. X. Ng, and L. Hanzo, "Unity-rate codes maximize the normalized throughput of on–off keying visible light communication," *IEEE Photonics Technology Letters*, vol. 29, no. 3, pp. 291–294, 2016.

[212] Z. Babar, M. A. M. Izhar, H. V. Nguyen, P. Botsinis, D. Alanis, D. Chandra, S. X. Ng, R. G. Maunder, and L. Hanzo, "Unary-coded dimming control improves ON-OFF keying visible light communication," *IEEE Transactions on Communications*, vol. 66, no. 1, pp. 255–264, 2017.

[213] J. Hu, M. Li, K. Yang, S. X. Ng, and K.-K. Wong, "Unary coding controlled simultaneous wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 637–649, 2019.

[214] M. El-Hajjar and L. Hanzo, "EXIT Charts for System Design and Analysis," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 127–153, 2014.

[215] L. Hanzo, O. Alamri, M. El-Hajjar and N. Wu, *Near-Capacity Multi-Functional MIMO Systems: Sphere-Packing, Iterative Detection and Cooperation.* John Wiley & Sons - IEEE Press, 2009.

[216] S. Ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE transactions on communications*, vol. 49, no. 10, pp. 1727–1737, 2001.

[217] J. Kliewer, N. Goertz, and A. Mertins, "Iterative source-channel decoding with Markov random field source models," *IEEE Transactions on Signal Processing*, vol. 54, no. 10, pp. 3688–3701, 2006.

[218] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for" turbo-like" codes," in *Proceedings of the annual Allerton Conference on Communication control and Computing*, vol. 36, pp. 201–210, University Of Illinois, 1998.

[219] G. D. Forney Jr, "Convolutional codes II. Maximum-likelihood decoding," *Information and control*, vol. 25, no. 3, pp. 222–266, 1974.

[220] J. A. Neasham, G. Goodfellow, and R. Sharphouse, "Development of the "Seatrac" miniature acoustic modem and USBL positioning units for subsea robotics and diver applications," in *Proceedings of IEEE OCEANS*, 2015.

[221] G. Heidari-Bateni and C. D. McGillem, "A chaotic direct-sequence spread-spectrum communication system," *IEEE Transactions on communications*, vol. 42, no. 234, pp. 1524–1527, 1994.

[222] G. Burel and C. Bouder, "Blind estimation of the pseudo-random sequence of a direct sequence spread spectrum signal," in *MILCOM 2000 Proceedings. 21st Century Military Communications. Architectures and Technologies for Information Superiority (Cat. No. 00CH37155)*, vol. 2, pp. 967–970, IEEE, 2000.

[223] R. Otnes, J. Locke, A. Komulainen, S. Blouin, D. Clark, H. Austad, and J. Eastwood, "Dflood network protocol over commercial modems," in *Proceedings of the Underwater Communications and Networking Conference (UComms'18)*, 2018.

[224] N. Morozs, P. Mitchell, and Y. Zakharov, "Unsynchronized dual-hop scheduling for practical data gathering in underwater sensor networks," in *Proceedings of IEEE UComms'18*, 2018.

[225] E. M. Sozer, M. Stojanovic, and J. G. Proakis, "Underwater acoustic networks," *IEEE journal of oceanic engineering*, vol. 25, no. 1, pp. 72–83, 2000.

[226] H. Song, C. Cho, W. Hodgkiss, S. Nam, S.-M. Kim, and B.-N. Kim, "Underwater sound channel in the northeastern East China Sea," *Ocean Engineering*, vol. 147, pp. 370–374, 2018.

[227] S. W. Golomb *et al.*, *Shift register sequences*. Aegean Park Press, 1967.

[228] S. W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar*. Cambridge University Press, 2005.

[229] P. Fan, M. Darnell, and M. Darnell, *Sequence design for communications applications*, vol. 1. Research Studies PressLtd, 1996.

[230] W. C. Lee, "Spectrum efficiency in cellular (radio)," *IEEE Transactions on Vehicular Technology*, vol. 38, no. 2, pp. 69–75, 1989.

[231] R. G. Maunder and A. Tavakkoli, "A communication unit for soft-decision demodulation and method therefor," Aug. 17 2023. US Patent App. 18/015,507.

[232] C. Brown and P. J. Vigneron, "Channel estimation and equalisation for single carrier continuous phase modulation," in *2011-MILCOM 2011 Military Communications Conference*, pp. 334–340, IEEE, 2011.

[233] S. Pasupathy, "Minimum shift keying: A spectrally efficient modulation," *IEEE Communications Magazine*, vol. 17, no. 4, pp. 14–22, 1979.

[234] K. Tani, Y. Medjahdi, H. Shaiek, R. Zayani, and D. Roviras, "PAPR reduction of post-OFDM waveforms contenders for 5G & Beyond using SLM and TR algorithms," in *2018 25th International Conference on Telecommunications (ICT)*, pp. 104–109, 2018.

[235] R. Koetter and A. C. Singer and M. Tuchler, "Turbo equalization," *IEEE Signal Processing Magazine*, vol. 21, pp. 67–80, Jan 2004.

[236] M. El Chamaa and B. Lankl, "Turbo-estimation for CPM over frequency-selective fast fading channels," *IEEE Transactions on Communications*, vol. 68, no. 4, pp. 2538–2550, 2019.

[237] A. Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Transactions on Communication Technology*, vol. 19, no. 5, pp. 751–772, 1971.

[238] 3GPP, "TR 25.212, Technical Specification Group Radio Access Network; Multiplexing and channel coding (FDD)," tech. rep., 3GPP, Mar 2022.

[239] J. Fischer, M. Grossmann, W. Felber, M. Landmann, and A. Heuberger, "A novel delay spread distribution model for VHF and UHF mobile-to-mobile channels," in *2013 7th European Conference on Antennas and Propagation (EuCAP)*, pp. 469–472, 2013.

[240] B. Sklar, "Rayleigh fading channels in mobile digital communication systems .I. Characterization," *IEEE Communications Magazine*, vol. 35, pp. 90–100, July 1997.

[241] C. Shannon, "The zero error capacity of a noisy channel," *IRE Transactions on Information Theory*, vol. 2, no. 3, pp. 8–19, 1956.

[242] J. Nieto, C. Brown, and P. Vigneron, "Achieving a Low Complexity, Power and Bandwidth Efficient Modulation Scheme for Land Mobile Communications," *NATO CIS CaP-LOS Comms CaT*, Aug 2014.

[243] M. El-Hajjar and L. Hanzo, "EXIT charts for system design and analysis," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 127–153, 2013.

[244] A. Hobbs and S. Holdcroft, "Venilia: Enabling Command and Control Using JANUS in Networked Underwater Environments," in *International Conference on Underwater Acoustics (ICUA 2022)*, 2022.

[245] K. McCoy, B. Tomasi, and G. Zappa, "Janus: The genesis, propagation and use of an underwater standard," *Proc. ECUA 2010*, 2010.

[246] NATO, *Sonar Acoustics Handbook*. NATO STO CMRE, 2016.

[247] M. Stojanovic, "On the Relationship Between Capacity and Distance in an Underwater Acoustic Communication Channel," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 11, no. 4, pp. 34–43, 2007.

[248] C. P. Shah, C. C. Tsimenidis, B. S. Sharif, and J. A. Neasham, "Low-complexity iterative receiver structure for time-varying frequency-selective shallow underwater acoustic channels using bicm-id: Design and experimental results," *IEEE journal of oceanic engineering*, vol. 36, no. 3, pp. 406–421, 2011.

[249] J. Heidemann, M. Stojanovic, and M. Zorzi, "Underwater sensor networks: applications, advances and challenges.," *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences*, vol. 370, no. 1958, pp. 158–75, 2012.

[250] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, "Toward the Development of Secure Underwater Acoustic Networks," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 1075–1087, 2017.

[251] M. Goetz, S. Azad, P. Casari, I. Nissen, and M. Zorzi, "Jamming-Resistant Multi-path Routing for Reliable Intruder Detection in Underwater Networks," in *Proceedings of the Sixth ACM International Workshop on Underwater Networks*, WUWNet'11, (Seattle, Washington, USA), December 1–2 2011.

[252] A. Signori, F. Chiariotti, F. Campagnaro, R. Petroccia, K. Pelekanakis, P. Paglierani, J. Alves, and M. Zorzi, "A Geometry-Based Game Theoretical Model of Blind and Reactive Underwater Jamming," *IEEE Transactions on Wireless Communications*, 2021.

[253] E. Souza, H. Wong, I. Cunha, A. Loureiro, L. Vieira, and L. Oliveira, "End-to-end authentication in under-water sensor networks," in *Proceedings of the 18th IEEE International Symposium on Computers and Communications*, ISCC'13, (Split, Croazia), pp. 299–304, July 7–10 2013.

[254] M. Zuba, M. Fagan, Z. Shi, and J.-H. Cui, "A Resilient Pressure Routing Scheme for Underwater Acoustic Networks," in *Proceedings of the 57th IEEE Global Communications Conference*, GLOBECOM'14, (Austin, TX, USA), December 8–12 2014.

[255] F. Campagnaro, D. Tronchin, A. Signori, R. Petroccia, K. Pelekanakis, P. Paglierani, J. Alves, and M. Zorzi, "Replay-Attack Countermeasures for Underwater Acoustic Networks," in *Global Oceans 2020: Singapore – U.S. Gulf Coast*, pp. 1–9, 2020.

[256] A. Munafo and G. Ferri, "An Acoustic Network Navigation System," *Journal of Field Robotics*, vol. 34, no. 7, pp. 1332–1351, 2017.

[257] L. A. Crum and Y. Mao, "Acoustically enhanced bubble growth at low frequencies and its implications for human diver and marine mammal safety," *The Journal of the Acoustical Society of America*, vol. 99, no. 5, pp. 2898–2907, 1996.

[258] L. S. Weilgart, "The impacts of anthropogenic ocean noise on cetaceans and implications for management," *Canadian journal of zoology*, vol. 85, no. 11, pp. 1091–1116, 2007.

[259] P. A. Van Walree, "Propagation and scattering effects in underwater acoustic communication channels," *IEEE Journal of Oceanic Engineering*, vol. 38, no. 4, pp. 614–631, 2013.

[260] W. D. Wilson, "Speed of Sound in Sea Water as a Function of Temperature, Pressure, and Salinity," *J. Acoust. Soc. Am.*, vol. 32, no. 6, pp. 641–644, 1960.

[261] B. Dushaw, "Worldwide Sound Speed, Temperature, Salinity, and Buoyancy from the NOAA World Ocean Atlas. http://staff.washington.edu/dushaw/WOA/," 2009.

[262] N. Morozs and W. Gorma and B. Henson and L. Shen and P. D. Mitchell and Y. Zakharov, "Channel modeling for underwater acoustic network simulation," *TechRxiv (submitted to IEEE Commun. Surveys Tuts.)*, Feb 2020.

[263] M. Porter, "Beam tracing for two- and three-dimensional problems in ocean acoustics," *J. Acoust. Soc. Am.*, vol. 146, no. 3, pp. 2016–2029, 2019.

[264] Y. Zakharov, B. Henson, R. Diamant, Y. Fei, P. Mitchell, N. Morozs, L. Shen, and T. Tozer, "Data Packet Structure and Modem Design for Dynamic Underwater Acoustic Channels," *IEEE J. Ocean. Eng.*, vol. 44, no. 4, pp. 837–849, 2019.

[265] F. Jensen, W. Kuperman, M. Porter, and H. Schmidt, *Computational Ocean Acoustics*. Springer, 2011.

[266] **Hamilton, Alexander**, J. Davies, and J. Neasham, "Phorcys open media layer specification (POMLS) for Progeny Task19WP2Y2," *Project 11708 – DEL2.4.1*, 2022.

[267] W. Jiang and R. Diamant, "Sparse channel estimation for long range underwater acoustic communication," in *2022 Sixth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2022.

[268] T. H. Glisson, C. I. Black, and A. P. Sage, "On sonar signal analysis," *IEEE Transactions on Aerospace and Electronic Systems*, no. 1, pp. 37–50, 1970.

[269] S. A. Kramer, "Statistical analysis of wide-band pseudorandom matched filter sonars," *IEEE Transactions on Aerospace and Electronic Systems*, no. 2, pp. 152–155, 1969.

[270] P. Bello, "Some techniques for the instantaneous real-time measurement of multipath and Doppler spread," *IEEE Transactions on Communication Technology*, vol. 13, no. 3, pp. 285–292, 1965.

[271] S. Soliman, "Synchronization issues in ocean telemetry," *IEEE journal of oceanic engineering*, vol. 16, no. 1, pp. 74–85, 1991.

[272] A.-M. Hobbs, J. Barnett, and **Hamilton, Alexander**, "Phorcys cryptographic Interoperability Specification (PCIS)," *DSTL/DOC133678 v1.0*, 2022.

[273] T. Corner, J. Neasham, and J. Davies, "Adaptive rake receiver performance for m-ary orthogonally modulated signals in the underwater acoustic channel," in *OCEANS 2023-Limerick*, pp. 1–8, IEEE, 2023.

[274] J.-P. Aumasson and D. J. Bernstein, "SipHash: A Fast Short-Input PRF," in *Progress in Cryptology - INDOCRYPT 2012* (S. Galbraith and M. Nandi, eds.), pp. 489–508, Springer Berlin, Heidelberg, 2012.

[275] M. J. Dworkin, *Recommendation for Block Cipher Modes of Operation:Methods for Key Wrapping (SP 800-38F)*. National Institute of Standards and Technology, Dec. 2012.

[276] K. J. Horadam, *Hadamard matrices and their applications*. Princeton university press, 2012.

[277] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," Tech. Rep. Federal Information Processing Standards Publications (FIPS PUBS) 140-2, Change Notice 2 December 03, 2002, U.S. Department of Commerce, Washington, D.C., 2001.

[278] D. J. Bernstein, *ChaCha, a variant of Salsa20*, pp. 84–97. Lecture Notes in Computer Science, Germany: Springer, 2008.

[279] A.-M. Hobbs and S. Holdcroft, *JANUS Class 17 "Venilia": Secure Pre-Canned Messaging*. Defence Science & Technology Laboratory, Fareham, Hampshire, June 2021.

[280] International Telecommunications Union, *G.704: Synchronous Frame Structures used at 1544, 6312, 2048, 8448 and 44,736 kbit/s Hierarchical Levels*, Oct. 1998.

[281] A.-M. Hobbs and S. Holdcroft, *Tiny Underwater Block cipher (TUBcipher): 27-bit Encryption Scheme for JANUS Class 17*. Defence Science & Technology Laboratory, Fareham, Hampshire, June 2021.

[282] L. Knudsen, G. Leander, A. Poschmann, and M. Robshaw, "PRINTcipher: A Block Cipher for IC-Printing," in *Cryptographic Hardware and Embedded Systems, CHES 2010* (S. Mangard and F.-X. Standaert, eds.), vol. 6225, pp. 16–32, 01 2010.

[283] L. B. VK5BR, "Underwater radio communication," *Originally published in Amateur Radio*, 1987.

[284] T. Melodia, H. Kulhandjian, L.-C. Kuo, E. Demirors, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, "Advances in underwater acoustic networking," *Mobile ad hoc networking: Cutting edge directions*, pp. 804–852, 2013.

[285] A. Song, M. Stojanovic, and M. Chitre, "Editorial Underwater Acoustic Communications: Where We Stand and What Is Next?," *IEEE Journal of Oceanic Engineering*, vol. 44, pp. 1–6, Jan 2019.

[286] A. Caiti, E. Crisostomi, and A. Munafò, "Physical Characterization of Acoustic Communication Channel Properties in Underwater Mobile Sensor Networks," in *Sensor Systems and Software* (S. Hailes, S. Sicari, and G. Roussos, eds.), (Berlin, Heidelberg), pp. 111–126, Springer Berlin Heidelberg, 2010.

[287] G. Ferri, A. Munafò, A. Tesei, P. Braca, F. Meyer, K. Pelekanakis, R. Petroccia, J. Alves, C. Strode, and K. LePage, "Cooperative robotic networks for underwater surveillance: an overview," *IET Radar, Sonar Navigation*, vol. 11, no. 12, pp. 1740–1761, 2017.

[288] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, "Toward the Development of Secure Underwater Acoustic Networks," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 1075–1087, 2017.

[289] J. Li, B. Yang, D. Ye, L. Wang, K. Fu, J. Piao, and Y. Wang, "A Real-Time, Full-Duplex System for Underwater Wireless Optical Communication: Hardware Structure and Optical Link Model," *IEEE Access*, vol. 8, pp. 109372–109387, 2020.

[290] A. Caiti, T. Fabbri, D. Fenucci, and A. Munafò, "Potential games and AUVs cooperation: First results from the THESAURUS project," in *2013 MTS/IEEE OCEANS - Bergen*, pp. 1–6, June 2013.

[291] F. Fabiani, D. Fenucci, and A. Caiti, "A distributed passivity approach to AUV teams control in cooperating potential games," *Ocean Engineering*, vol. 157, pp. 152 – 163, 2018.

[292] V. Yordanova, H. Griffiths, and S. Hailes, "Rendezvous planning for multiple autonomous underwater vehicles using a Markov decision process," *IET Radar, Sonar Navigation*, vol. 11, no. 12, pp. 1762–1769, 2017.

[293] D. P. Eickstedt and S. R. Sideleau, "The backseat control architecture for autonomous robotic vehicles: A case study with the Iver2 AUV," *Marine technology society journal*, vol. 44, no. 4, pp. 42–54, 2010.

[294] J. Alves, T. Furfaro, K. LePage, A. Munafò, K. Pelekanakis, R. Petroccia, and G. Zappa, "Moving JANUS forward: a look into the future of underwater communications interoperability," in *OCEANS 2016 MTS/IEEE Monterey*, pp. 1–6, IEEE, 2016.

[295] J. Alves, T. Furfaro, K. LePage, A. Munafò, K. Pelekanakis, R. Petroccia, and G. Zappa, "Moving JANUS forward: A look into the future of underwater communications interoperability," in *OCEANS 2016 MTS/IEEE Monterey*, pp. 1–6, 2016.

[296] CMRE, *Janus Wiki*, (accessed March, 2023). http://www.januswiki.com/tiki-index.php.

[297] R. Petroccia, J. Alves, and G. Zappa, "JANUS-Based Services for Operationally Relevant Underwater Applications," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 994–1006, 2017.

[298] M. S. Afaqui, E. Garcia-Villegas, and E. Lopez-Aguilera, "IEEE 802.11ax: Challenges and requirements for future high efficiency WiFi," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 130–137, 2017.

[299] R. Petroccia and D. Spaccini, "Comparing the SUNSET and DESERT frameworks for in field experiments in underwater acoustic networks," in *Proceedings of IEEE OCEANS'13*, pp. 1–10, June 2013.

[300] H. S. Dol, P. Casari, T. Van Der Zwan, and R. Otnes, "Software-defined underwater acoustic modems: Historical review and the NILUS approach," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 3, pp. 722–737, 2016.

[301] D. Green, J. Dellamorte, and J. Dellamorte, "Enhancing JANUS signaling," in *2021 Fifth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, IEEE, 2021.

[302] R. Petroccia, F. Ferreira, J. Alves, B. Cardeira, G. Zappa, V. Manzari, G. Cario, J. DellaMorte, K. Ehmcke, O. Kebkal, *et al.*, "The 2019 JANUS interoperability fest: A field report," *Marine Technology Society Journal*, vol. 55, no. 2, pp. 5–16, 2021.