Using Coding to Improve Localization and Backscatter Communication Performance in Low-Power Sensor Networks

by

Itay Cnaan-On

Department of Electrical and Computer Engineering
Duke University

Date: _____

Approved:

_____
Jeffrey Krolik, Co-supervisor

_____
Robert Calderbank, Co-supervisor

_____
Matthew Reynolds

_____
Henry Pfister

_____
Loren Nolte

Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Department of Electrical and Computer Engineering in the Graduate School of Duke University
2016

Abstract

Using Coding to Improve Localization and Backscatter Communication Performance in Low-Power Sensor Networks

by

Itay Cnaan-On

Department of Electrical and Computer Engineering
Duke University

Date: _____

Approved:

_____
Jeffrey Krolik, Co-supervisor

_____
Robert Calderbank, Co-supervisor

_____
Matthew Reynolds

_____
Henry Pfister

_____
Loren Nolte

An abstract of a dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Department of Electrical and Computer Engineering
in the Graduate School of Duke University
2016

Copyright © 2016 by Itay Cnaan-On
All rights reserved except the rights granted by the
Creative Commons Attribution-Noncommercial Licence

Abstract

Backscatter communication is an emerging wireless technology that recently has gained an increase in attention from both academic and industry circles. The key innovation of the technology is the ability of ultra-low power devices to utilize nearby existing radio signals to communicate. As there is no need to generate their own energetic radio signal, the devices can benefit from a simple design, are very inexpensive and are extremely energy efficient compared with traditional wireless communication. These benefits have made backscatter communication a desirable candidate for distributed wireless sensor network applications with energy constraints.

The backscatter channel presents a unique set of challenges. Unlike a conventional one-way communication (in which the information source is also the energy source), the backscatter channel experiences strong self-interference and spread Doppler clutter that mask the information-bearing (modulated) signal scattered from the device. Both of these sources of interference arise from the scattering of the transmitted signal off of objects, both stationary and moving, in the environment. Additionally, the measurement of the location of the backscatter device is negatively affected by both the clutter and the modulation of the signal return.

This work proposes a channel coding framework for the backscatter channel consisting of a bi-static transmitter/receiver pair and a quasi-cooperative transponder. It proposes to use run-length limited coding to mitigate the background self-interference and spread-Doppler clutter with only a small decrease in communication rate. The

proposed method applies to both binary phase-shift keying (BPSK) and quadrature-amplitude modulation (QAM) scheme and provides an increase in rate by up to a factor of two compared with previous methods.

Additionally, this work analyzes the use of frequency modulation and bi-phase waveform coding for the transmitted (interrogating) waveform for high precision range estimation of the transponder location. Compared to previous methods, optimal lower range sidelobes are achieved. Moreover, since both the transmitted (interrogating) waveform coding and transponder communication coding result in instantaneous phase modulation of the signal, cross-interference between localization and communication tasks exists. Phase discriminating algorithm is proposed to make it possible to separate the waveform coding from the communication coding, upon reception, and achieve localization with increased signal energy by up to 3 dB compared with previous reported results. The joint communication-localization framework also enables a low-complexity receiver design because the same radio is used both for localization and communication.

Simulations comparing the performance of different codes corroborate the theoretical results and offer possible trade-off between information rate and clutter mitigation as well as a trade-off between choice of waveform-channel coding pairs. Experimental results from a brass-board microwave system in an indoor environment are also presented and discussed.

The thesis is dedicated to my wife, Noa, my daughter Inbal and my son Amit for the love and happiness they give me. This work is also dedicated to my parents, Natan and Mira, who thanks to their love, support and dedication I have become what I am today.

Contents

Abstract **iv**

List of Tables **xi**

List of Figures **xii**

List of Abbreviations and Symbols **xvi**

Acknowledgements **xviii**

1 Introduction to Backscatter Communication **1**

1.1 Point-to-Point Wireless Communication 1

1.2 Historical Origin of Backscatter Communication 5

1.3 Backscatter Communication - Concept and Topology 7

1.4 RF Tags Concept of Operation 9

1.5 Backscatter Communication - A System Overview 12

1.6 Signal Impairments of Backscatter Communication 13

2 Communication Processing **14**

2.1 CW signal processing overview 14

2.2 FMCW signal processing overview 15

2.2.1 Comparison of Processing of FMCW and CW 18

2.2.2 FMCW as a Spread-Spectrum 19

2.2.3 FMCW Pulse-to-Pulse Coherence Effect on Receiver Utilization 19

2.3 Signal Model of Backscatter Communication with FMCW 20

2.4 Receiver Processing of Backscatter Communication with FMCW . . . 23
2.4.1 De-chirp Process (De-mix of radar pulse) 24
2.4.2 Demodulating the Range Induced Carrier 24
2.4.3 Matched Filtering to Recover Node Symbols 25
2.5 Coding Utilization for Clutter Filtering with FMCW 26
2.5.1 Clutter Reflections Model in CW and FMCW 26
2.5.2 Modeling Clutter as Cyclo-Stationary Process in FMCW . . . 28
2.5.3 Algorithm 1, Line-Coding Across Exact Neighboring Chirps . 29
2.5.4 Algorithm 2, Differential Line-Coding 30
2.6 Backscatter Communication Multiple Access and Collision Avoidance 31
2.6.1 Multiple Access with FMCW 33
2.6.2 Upper Bound on Node Spatial Density and Node Data Rate using FMCW 35
2.7 Multipath Propagation Analysis in CW and FMCW 35
2.7.1 Backscatter Communication Multipath Mitigation Overview . 37
2.7.2 Modeling of Multipath Reflections in FMCW 38
2.7.3 Use of Spectral Filtering for Partial Mitigation of Multipath in FMCW 38
2.8 Experimental Results 38
2.8.1 Single Node In View 40
2.8.2 Multiple Nodes in View 42
3 Localization **45**
3.1 Localization Processing with FMCW 45
3.1.1 Enhanced Range Accuracy through Slow Rate Modulation . . 46
3.2 FMCW Localization Performance Analysis Through the Averaged Cross-Ambiguity Function 48

3.2.1 Phase Modulated Baseband Averaged Power Spectral Density (PSD) . . . 51

3.3 Fisher Information and the Cramér-Rao Lower Bound (CRB) 53

3.3.1 Fisher Information on Ranging at the De-Chirped Processing Output . . . 56

3.3.2 Signal Model of the De-Chirped Processing Output . . . 57

3.3.3 Fisher Information on Carrier Frequency Estimation of Linear Modulation . . . 58

3.3.4 Development of the Fisher Information and Cramér-Rao Lower Bound (CRB) for Localization of FMCW with Modulated Backscatter . . . 60

3.4 Cramér-Rao Lower Bound (CRB) and Maximum-Likelihood Estimator for Localization of FMCW with Modulated Backscatter . . . 61

3.4.1 CRB for the Case of Modulation Rate Is Zero . . . 62

3.4.2 Evaluation of the Fisher Information for the Case of Modulation Rate Is Zero . . . 62

3.4.3 CRB for the Case of Message Known to Reader (Pilot/Preamble) 65

3.4.4 Evaluation of the Fisher Information for the Case of Message Known to Reader . . . 65

3.4.5 CRB for the Case of Message Unknown to Reader . . . 68

3.4.6 Evaluation of the Fisher Information for the Case of Message Unknown to Reader . . . 69

4 Quasi-Cooperative Range and Channel Coding 73

4.1 Introduction . . . 73

4.2 Backscatter communication channel model and signal processing . . . 76

4.2.1 Backscatter communication processing overview . . . 76

4.2.2 Clutter and fading in backscatter communication . . . 79

4.2.3 Self-interference . . . 79

4.2.4 Spread-Doppler clutter . . . 80

4.3 Doppler run length limited channel coding 82
4.3.1 RLL codes overview 82
4.3.2 Doppler RLL encoding setup 83
4.3.3 Doppler RLL decoding setup 84
4.3.4 Extension to QAM symbols 86
4.3.5 Clutter rejection by using RLL codes 88
4.4 Waveform coding for high resolution range estimation 90
4.4.1 Waveform coding and time-delay estimation setup 91
4.4.2 Time-delay estimation analysis 94
4.4.3 The effect of tag modulation on time-delay estimation 95
4.4.4 Frequency waveform coded interrogation signals 96
4.4.5 Asymmetric bi-phase waveform coded interrogation signals . . 101
4.4.6 Symmetric bi-phase waveform coded interrogation signals . . . 103
4.4.7 Ranging with frequency and phase coded interrogation signals - simulation results 109

5 Conclusions and Future Work **112**

5.1 Conclusions 112
5.2 Future work - Optimal codes for backscatter communication channel . 113
5.3 Future work - Multi-phase waveform codes for backscatter communication 114

Bibliography **115**

Biography **121**

List of Tables

2.1 Example FMCW Backscatter Link Budget 44

List of Figures

1.1 An illustration showing the use of semaphore line. Source: wikipedia.com 6

1.2 A use of the heliograph. Source: wikipedia.com 7

2.1 The LFM waveform envelope with pulse duration $T = 1\ s$ and bandwidth $B = 100\ Hz$ 16

2.2 Example FMCW backscatter communication system 17

2.3 Block diagram of system and signal processing framework 18

2.4 Simulated clutter return in FMCW system, when observed after dechirping the radar pulse 28

2.5 Simulated baseband spectrum for the line coding of algorithm 1 with (a) $M = 2$ and no coding for comparison, and (b) $M = 8$ 29

2.6 Differeential Line-coding technique for clutter mitigation 31

2.7 Simulation and analyical results of decoded signal using differential Line-coding. Decision region boundaries are marked as dashed lines. . 32

2.8 Simulated received power spectrum of node transmitting at rate $1/T_b =$ 10 kHz at range of 15 m corresponding to a range subcarrier of 20 kHz 34

2.9 Simulated baseband energy spillover between adjacent nodes 34

2.10 Measured eye diagram for RF tag backscatter 37

2.11 Photograph of experimental radar setup in 60 m indoor hallway . . . 39

2.12 Measured power spectrum of received signal before (light) and after (dark) clutter filtering with node signal is centered around subcarrier of $f_i = 40$ kHz, parameters used: f_c=2.45 GHz, B=40 MHz, T_p=20 ms, T_b=40 ms 41

2.13 Measured received signal waveform after removal of range induced carrier and clutter (dark) and transmitted signal waveform (light), parameters identical to Fig. 2.12 41

2.14 Measured received power spectrum of two nodes simultaneously transmitting (top), filtered baseband power spectrum of nodes after range separation (middle row) and recovered data waveform versus transmitted signal waveform prior to matched filtering (bottom row) . . . 42

2.15 Measured eye diagram for (a) node at 15 m and (b) node at 33 m . . 43

3.1 Measured amplitude-range-Doppler surface plot (dB) recovered from a node at 4 m sending the preamble (1010...) at $1/T_b = 10$ Hz and a chirp rate of $1/T_p = 1$ kHz 47

3.2 An ambiguity function of LFM pulse 49

3.3 Cross ambiguity function of backscatter communication 51

3.4 ACAF of different symbol sequences (assuming $M = 8$ symbols per radar pulse) 52

3.5 ACAF of different radar FM frequnecty sweep rate 53

3.6 ACAF of different symbols rate 53

3.7 ACAF of different symbol modulation scheme 54

3.8 Validation against experimetnal results with parameters described in chapter 3 54

3.9 Modulated range induced carrier 59

3.10 Case of modualtion rate is zero 64

3.11 Estimator approximating the MLE 67

3.12 Case of constant message sent 67

3.13 Estimator approximating the MLE 71

3.14 Case of modulation unknown to reader 72

4.1 Backscatter communication between RF tag and a reader with common channel interferences 75

4.2 Processing chain of simultaneous communication and time-delay estimation. 77

4.3 Delay-Doppler simulation of a signaling RF tag coded with RLL(1,3) across pulses (seen as the symmetric concentrations around $+/-$ 1000 Hz) and added spread-Doppler clutter (<200 Hz) at arbitrary power (seen as a narrow band around the Doppler DC). The RLL Doppler code shapes the Doppler spectrum of the tag and pushes it away from the clutter. Scale is in dB. 82

4.4 Run-length limited Doppler encoding and decoding process 83

4.5 RLL coding for quadrature phase shift keying modulation. 87

4.6 Spectrum of selected run-length limited codes before (upper row) and after (lower row) the inverse NRZI subtraction operation. 88

4.7 Spectrum of Doppler run-length limited code $(1, 3)$ driving a rectangular pulse after the inverse NRZI subtraction operation (red). Static clutter returns shows as lines (black). At the back (blue), a reference of uncoded random data with rectangular pulse and no subtraction operation. The coded spectrum exhibits notches that appear at integer multiples of the pulse repetition frequency, where clutter is dominant. 89

4.8 figure 91

4.9 A comparison of robustness to spread-Doppler self-interference bandwidth of various RLL codes. Simulation parameters: averaged over 5000 iterations, clutter model is composed of $1:1$ energy ratio of static and spread-Doppler, $E_s/P_{clutter} = -20$ dB, no noise added. . . . 92

4.10 A comparison of robustness to spread-Doppler self-interference clutter together with additive white Gaussian noise. Z-axis represents the BER. Simulation parameters: averaged over 100 iterations, clutter model is composed of $1:1$ energy ratio of static and spread-Doppler,clutter bandwidth is < 5 Hz. 93

4.11 Symbols constellation demonstrates a phase mirror impairment. The phase ambiguity is caused when a reader waveform code is using a bi-phase phase shift-keying (BPSK) and RF tag is using BPSK as well. 97

4.12 Symbols constellation demonstrates a phase mirror impairment. The phase ambiguity is resolvable when a reader waveform code is using a asymmetric bi-phase phase shift-keying (BPSK) and RF tag is using BPSK. 104

4.13 Simulation results of phase remapping for reader waveform using a asymmetric bi-phase phase shift-keying (BPSK) Golomb15 code and RF tag is using BPSK and random i.i.d symbols modulation. Additive white Gaussian noise at SNR=30 dB. (a) Before receiver front end subtraction (b) After subtraction, notice the increase of noise variance due to the subtraction operation. (c) After receiver remapping. 105

4.14 Time diagram of the signals at the receiver. The receiver has uncertainty in time-delay τ and symbol phase ϕ, yet after processing the waveform code is reconstructed. 107

4.15 RF-tag embeds quasi-cooperative code sequences into data stream, and allows time-sharing between data and ranging support sequences. 108

4.16 A comparison of time-delay estimation error between different waveform coding as a function of the ratio of quasi-cooperative coding. . . 110

4.17 A comparison of time-delay estimation error between different waveform coding as a function of SNR. 111

List of Abbreviations and Symbols

Abbreviations

ACAF	Average complex ambiguity function
ACF	Autocorrelation function
AWGN	Additive white Gaussian noise
BER	Bit error rate
BPSK	Binary phase shift keying
CRB	Cramer-Rao bound
CW	Continuous wave
EM	Electromagnetic
FMCW	Frequency modulated continuous wave
IF	Intermediate frequency
IWC	Interrogation waveform code
LFM	Linear frequency modulation
MLE	Maximum likelihood estimator
MTI	Moving target indication
NRZI	Non-return to zero inverted
PRF	Pulse repetition frequency
PSK	Phase shift keying
QAM	Quadrature amplitude modulation
QCC	Quasi-cooperative code

QPSK	Quadrature phase shift keying
RF	Radio frequency
RLL	Run-length limited
SCNR	Signal to clutter plus noise ratio
SNR	Signal to noise ratio

Acknowledgements

I wish to thank my committee members who shared with me their wisdom and expertise. Special thanks to my committee co-chairs Dr. Jeff Krolik and Dr. Robert Calderbank, for their mentoring, reflection and good advice along the way. I was fortunate to work with them and discover the world of signal processing and coding. I also would like to thank Dr. Matt Reynolds for his guidance and for teaching me the magic of closing the gap between theory and practice. Thanks to Dr. Henry Pfister for showing me how to see creative approaches to difficult problems. Thanks also to Dr. Loren Nolte for his useful discussions and providing a holistic view of the problem domain.

I would also like to thank Dr. Andrew Harms for the long hours of turning ideas together from a sketch on a white board into a publishable papers. Thanks also to Dr. Stewart Thomas for the long days of turning symbols on a paper into actual radio signals that manifest over the air, and for teaching me the ability to get things done.

I would like to acknowledge and thank the National Science Foundation and Office of Naval Research for their financial support throughout my journey. Thanks to Dr. Silvia Ferrari, for supporting me through the Wireless Intelligent Sensor Networks initiative in Duke. Thanks also goes to Duke University Electrical and Computer Engineering department for the provided financial support.

I would also like to express my thanks to other universities I have interacted with.

Thanks to the Institute of Microwave and Photonics at the University of Erlangen-Nurnberg, Germany for hosting me as visiting researcher, and special thanks to the chair Dr.-Ing. Martin Vossiek. Thanks also for University of Washington and especially Dr. Matt Reynolds for hosting me for an intensive joint field experiment.

In addition, I would like to thank Tel-Aviv University, as the place who gave me the solid engineering foundations and great education for the journeys ahead.

Lastly, I am grateful for my wonderful wife and partner in life, Noa, who believed in me throughout this journey of graduate studies and the writing of this dissertation. She gave me good advice, discussed ideas and gave me support and love when I needed them most. I couldn't have done it without her.

1

Introduction to Backscatter Communication

1.1 Point-to-Point Wireless Communication

We approach backscatter communication methodically through highlighting its differences from the traditional point-to-point communication. We turn first to describing the fundamentals of point-to-point communication, as it will serve to demonstrate some of its limitations and similarities with backscatter communication.

Point-to-point wireless communication has been developed based on the discovery and harnessing of the physical phenomenon of Electromagnetic (EM) wave propagation. Electromagnetic wave propagation has been used for almost 150 years now for wireless data communication, where Data is conveyed by modulating (altering) one or more properties of an EM waveform. Waveform parameters that are commonly used for such purposes are amplitude, frequency, phase, and polarization (see Proakis (2000)).

The topology of a point-to-point wireless communication in its most basic form

consists of two dimensionless nodes in a simplex form: a transmitter that is interested in conveying its data, and a receiver who is interested in receiving the data. The transmitter contains a data source that generates an electronic signal containing the data, an EM waveform generator that creates the basic waveform to be propagated and a modulation unit that alters some properties of the EM waveform to reflect changes in the data signal. The receiver has a demodulation unit used to separate the data signal from the EM waveform and a data processing unit used to process the data from its electronic data signal.

Another principal topology of point-to-point wireless communication is the bi-directional (duplex) topology. In this topology two nodes are both interested in conveying data to each other and also to receive data from each other. Functionally, each node has all the functions of a receiver and all the functions of transmitter, also dubbed transceiver.

Other types of wireless communication topologies involve multi-nodes communication. For example star, mesh, ring and tree are some examples. In general, multi-node topologies can be viewed as specific cases of the more general bi-directional (duplex) or simplex communication frameworks, although they involve unique signal impairments and synchronization problems.

The use of point-to-point communication brings signal impairments which challenge the ability of the receiver to process the signal correctly and reconstruct the sent data:

1. **Attenuation** such that the signal power is attenuated according to free-space path loss using Friis transmission equation (1.1) (see Friis (1946)).

$$\frac{P_r}{P_t} = G_t G_r (\frac{\lambda}{4\pi R})^2 \tag{1.1}$$

where P_r is the power at the receive antenna, P_t is the power at the transmit antenna, G_t and G_r are the antenna gain for the transmit and the receive antenna respectively, λ is the wavelength and R is the distance between the antennas.

2. **Thermal noise** which appears at the receiver as a result of thermal agitation of the electrons. In an ideal receiver, this noise is uncorrelated with itself (white) and uncorrelated with any of the other communication signals (i.e. EM waveform, data signal). The noise power is linear with the temperature (see Lathi (1998)).

3. **Multipath propagation/ Inter-symbol interference** which happens when the transmitted signal reaches the receiver by more than one propagation path as a result of reflection from intermediate objects. The resulting received signal is an overlap of all multi-path signal copies, each with different delay corresponding to the path traveled. In the perspective of symbols, one symbol can overlap an earlier symbol with a shorter delay. This interference is highly correlated with the transmitted signal (see Lathi (1998)).

4. **Crosstalk** which are other sources of EM waves, such as other communication systems, natural EM sources, etc. These interferences can be partially correlated with the transmitted signal, for example if similar signal characteristics such as the frequency or modulation scheme are similar to the signal of interest (see Johnson and Sethares (2004)).

5. **Synchronization** which is required between the transmitter and receiver, so that the receiver can process the incoming signal with less uncertainty on some of the signal parameters (e.g. carrier phase).

The Superheterodyne transmitter/receiver structure is a widely used hardware

architecture developed almost 100 years ago to allow flexibility and simplicity in the design of receivers. The architecture employs the signal processing concept of Heterodyning or frequency mixing. A mixer, usually a transistor and formerly a vacuum tube, would mix two signals at frequencies f_1 and f_2, creating two new signals, one at the sum of the frequencies $f_1 + f_2$ and the other at the difference of the frequencies $f_1 - f_2$, also dubbed 'beat frequency'.
This principle allows to design a receiver/transmitter that operates at some intermediate frequency (IF) f_1 which is different (usually lower) than the radio frequency (RF) that is actually being sent over the air $f_1 + f_2$, and being determined dominantly by the carrier frequency f_2. The benefits of this separation is better flexibility in design of adjustable carrier frequencies, simpler filtering in lower frequency band (IF) and less expensive hardware, now required to operate in a lower frequency band (IF) (see Proakis et al. (1994)).

With the advances in hardware, communication devices became smaller and cheaper to fabricate, creating a set of new application and use cases. One of the major key aspects limiting the use of mobile device communication is the stringent restriction of local energy storage and energy consumption rate. The research area of efficient energy consumption communication is still an open research question with a very active community spanning from materials engineering to advance batteries storage capacity, efficient communication protocols with low overhead, efficient hardware design (circuits that shuts themselves when not in use) and new signal processing algorithms (sparse FFT) (see Bi et al. (2001)). Battery technology is limiting the local energy storage as devices become smaller. Efficient consumption of energy or energy policy usage might lengthen the operation of a device before a new source of energy is installed or charging the depleted one. Hitherto, several communication protocols have provided lower profile of communication with a goal of trading some

of the properties of communication (such as range of operation, communication rate, latency etc.) with better usage of the energy resource. For example ZigBee protocol (IEEE 802.15.4 standard) uses the presence of spatially spread nodes to provide efficient low-power multi-hop communication. Another example is Bluetooth low energy (BLE) providing longer device lifetime operation on the expense of range and communication rate.

1.2 Historical Origin of Backscatter Communication

The first reliable indication of a communication system being energized and activated by an outside energy source to convey information was first introduced in 1792 in France by Claude Chappe. The system, called 'Napoleonic Semaphore' or the 'semaphore telegraph', consisted of a network of towers each with pivoting mechanical shutters, where information was encoded in the position of the shutters (see Fig. 1.1). The system only functioned during the day and weather conditions permitting good visual sight, relying entirely on the sun as an optical source of energy (see Burns (2004)).

A later development from 1821 by Carl Friedrich Gauss in Göttingen, invented the Heliograph (In Greek, 'helios' means sun and 'graphein' meaning 'write'), which was also based on optics. The concept uses a mirror with built-in shutter to reflect the sun beam towards and away from the receiver, thus creating a pattern of flashes encoding the information message (see Burns (2004) and Fig. 1.2).

Moving from the optical domain into radio signals, from 1935 and throughout World War II, Germany and Britain used the technology of Identification Friend or Foe (IFF) to distinguish friendly aircraft from enemy in the radar's received signal. In this case, the outside energy source is a radar, emitting powerful EM waves. The friendly aircraft is equipped with a device called 'transponder' which reflects

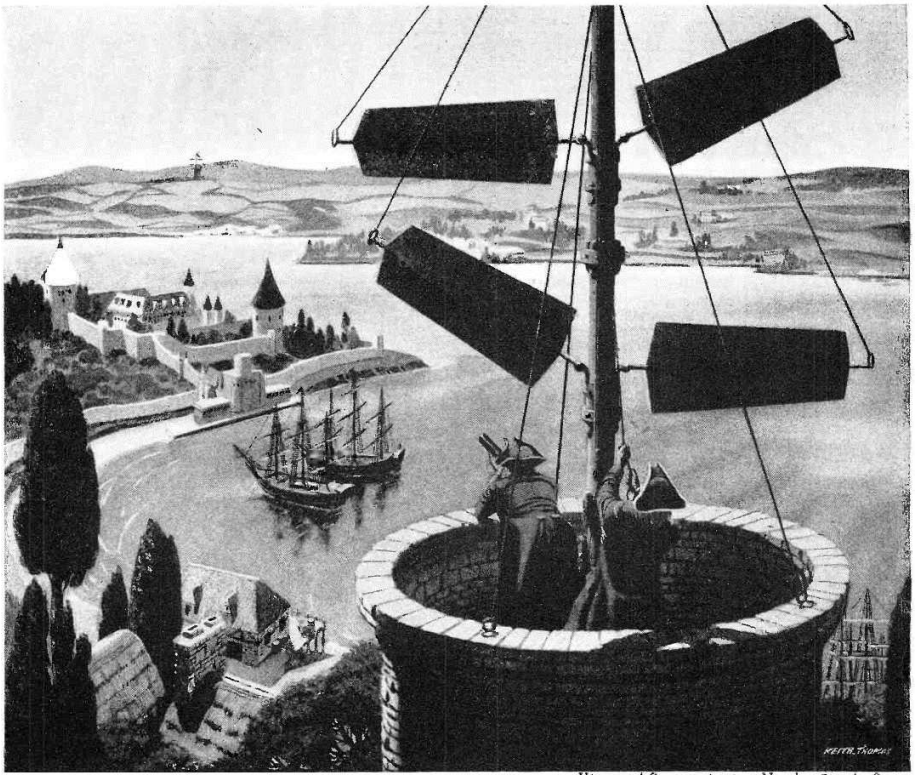


FIGURE 1.1: An illustration showing the use of semaphore line. Source: wikipedia.com

and modulate the backscatter radar signal with a unique signature which encodes 'friend'. The radar processes the received modulated signal and for each target extracts if the unique signature was sent or not. It is worth mentioning the use of two types of transponders: 'passive', which simply modulates the reflected backscatter with the signature and 'active', which also performs other changes to the backscatter signal (e.g. increasing amplitude, adding delay) (see Greg (2015)).

In 1948, a seminal paper by Harry Stockman laid down the foundations of backscatter communication, describing it as 'Communication by means of reflected power'. The paper provided an analysis and the experiential results from the perspective of a radar. It mostly concerns power calculations and hardware design of the

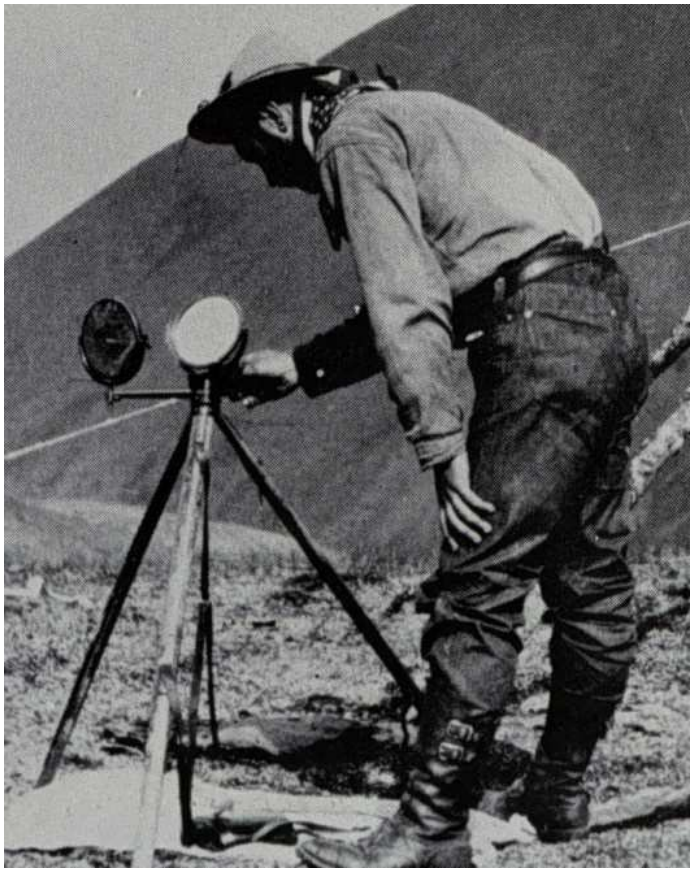


FIGURE 1.2: A use of the heliograph. Source: wikipedia.com

reflectors, while modulation is performed using a mechanical oscillation (see Stockman (1948)).

1.3 Backscatter Communication - Concept and Topology

Backscatter wireless communication has been developed based on the discovery and harnessing of the physical phenomenon of Electromagnetic (EM) backscatter. Electromagnetic backscatter is a physical phenomenon describing a reflection of an EM waveform back towards the direction from which it come. Since the reflecting object is in most cases not perfectly uniform, a specular reflection, such that follows a perfect mirror-like reflection, cannot be assumed. Rather, a scattering of the waveform

will occur and diffuse reflection will result in reflections in multiple angles (see Griffiths and College (1999)).

In a backscatter communication set-up, the source of the data is not the same as the source of the EM waveform (as is the case with point-to-point communication). An EM waveform source generates waveforms that propagate and illuminate the surroundings, scattering and reflecting from objects around. An object residing in that surrounding (often times called 'transponder' or 'RF tag') can convey/signal data by altering (modulating) the backscatter reflections scattering from it. A receiver residing in the same surrounding can receive the modulated reflections bouncing off the object, process them and extract the underlying data encoded in the signal.
It is important to distinguish between two variants of backscatter communication:

- **Mono-static topology -** The receiver is also the source of the EM waveform. The receiver in this topology is sometimes called 'interrogator' (see EPC Global US (2005)) or 'reader'. It is assumed that all parameters of the EM waveform signal (signal pattern, frequency, phase etc.) are known to the receiver. A slightly different version of this topology called 'co-located' topology, has the transmitter and receiver very closely located but separated, regardless of how they are synchronized.

- **Bi-static topology -** The receiver is independent and separated by physical distance from the source of the EM waveform. Notice that literature sometime refers also to the receiver in this topology as 'reader'. This topology is also called 'Ambient backscatter' (see Liu et al. (2013)) and in most cases the EM source is non cooperative with the receiver, such that the receiver has less

knowledge about the EM waveform (e.g. signal phase, specific signal pattern).

The focus of this work is on mono-static topology for the following reasons. First, this topology is more established in terms of a well defined problem domain tied with real world applications, it also focuses most of the research and has a solid body of research work that is validated with elaborate experiments and industry applications. Second, in order to handle impairments of the signal and especially multi-path propagation (see section 2.7), it is better to be able to design an algorithm that can incorporate exact knowledge and control over the transmitted signal. In a sense of estimation theory, the estimation of parameters of interest (such as the data of the RF tag signal) would become harder as there is more uncertainty present in the problem (ambiguity about parameters of the EM waveform such as phase or amplitude for example) (see Kay (1993)). Third, when designing a communication system, it is often desired to have control of the serviced coverage area and reliability. Relying on an outside emitter, or illuminators of opportunity, could limit the ability to provide robust service coverage level.

Conceptually, backscatter communication can be perceived as a process of **data harvesting**, where multiple RF tags are constantly 'sprouting' new data, the reader is collecting the data by beaming a waveform into the field, where the reflection comes back with the 'harvested' data to the reader.

1.4 RF Tags Concept of Operation

Key operation of backscatter communication lies in the ability of the remote RF tag to signal valuable data by modulating the reflected backscatter. To that end, the modulation can be achieved using controlled alteration of the **reflection coefficient** of the RF tag. The reflection coefficient is defined as a complex ratio of the reflected

wave to that of the incident wave

$$\Gamma = \frac{E^-}{E^+} \tag{1.2}$$

Another perspective for the modulation of the reflection coefficient can be viewed in a change of the **radar cross-section (RCS)** of the RF tag (see Yen et al. (2007)). This perspective will be useful when analyzing the RF tag modulation in terms of radar localization performance in chapter 3.

The RF tag does not require to have a transmitter or amplifier hardware as in point-to-point communication. Instead, the alteration of the reflection coefficient can be implemented by switching between discrete loads connected to the RF tag's antenna (see Thomas et al. (2012)) to generate desired phase or amplitude modulated symbol. Alternatively, a phase shift module connected to the antenna can also generate phase or amplitude modulated symbols (see Winkler et al. (2010)). The effectively generated modulation will therefore be either Amplitude-shift keying (ASK) or Phase-shift Keying (PSK). The RF tag does not need to know the exact operating bandwidth of the EM transmitter, which makes the system design and change of EM parameters easier. As long as the reader uses a frequency band which is matched to the antenna and the microwave circuitry of the tag, the tag frequency response should be indifferent to the interrogator frequency. However, when the frequency band used by the reader is larger than the tag hardware frequency operation range, this will cause incoherent attenuation and mismatch across the bandwidth that needs to be considered in the design of the system.

There are three major classes of RF tags, defined by their method of operation:

- **Passive -** relying entirely on passive scattering, usually when the data does not change over time (e.g. serial identification number as in RFID)

- **Battery assisted passive -** fed by a local source of energy such as a capacitor or battery which is used to operate local electronics/circuitry/micro-controller to handle dynamic data (such as a sensor's readings) that needs to be signaled and the modulating signal. Energy consumption is considered ultra-low power compared with transmitter equipped device, and can operate for very long durations of time, in the order of years (see Polastre et al. (2005)). This class is also sometimes called 'semi-passive'.

- **Active -** employs a transmitter, similar to point-to-point communication devices. It's source of energy is fed by local battery, and energy consumption is relatively high (see Polastre et al. (2005)). This allows for further processing of the signal and higher signal to noise ratios (SNR) compared with the semi-passive or passive methods of operation.

The very low profile demand on energy required for the operation of semi-passive or active RF tags makes them a perfect candidate to be paired with **energy harvesting** techniques to achieve a totally battery-free communication system. Such property is naturally highly desirable for a communication system. Energy harvesting is a process that allows a device to extract energy from an external source such as solar power, heat, acoustic vibrations or EM source (see Priya and Inman (2009)), consume it immediately or store it locally (in a capacitor or a battery) for later use. Extensive research has targeted the area of energy harvesting for the operation of semi-passive tags with notable achievements (see Liu et al. (2013)). However, it is important to stress out that the amount of energy collected is relatively small, and there is a great dependence on the distance from the EM source which limits the range of operation to an order of magnitude less than using semi-passive or active RF tags.

1.5 Backscatter Communication - A System Overview

When considering a communication system as a whole, backscatter communication has certain advantages over point-to-point communication. Considering the communicating node and receiver in point-to-point communication, the backscatter topology allows to offset energy, circuitry, complexity, size, cost and processing required for communication to the receiver on the expense of the signaling node. This makes sense for a system when the number of tags is an order of magnitude larger than the number of readers.

Some system comparisons of backscatter and point-to-point communication:

- Low cost of nodes when the need is for a large number of nodes and relatively small number of readers. The simple design of an RF tag with small amount of hardware elements compared with a regular communication node (transmitter, amplifier, battery etc.), makes the average cost per tag significantly lower. For example, RF tags used for retail inventory are passive and carry only a serial number (RFID). Their numbers are in the order of thousands or even millions while the number of readers is usually in the order of hundreds (see Chawla and Ha (2007)).

- Low energy consumption of nodes allows for the operation of nodes for extended duration of time without servicing. There is no use of any local energy (in passive RF tags), or ultra low power consumption (in semi-passive RF tags) using local battery or capacitor for use during the entire lifetime (no replacement or charging of battery).

- Smaller form factor as there are less hardware elements.

- Smaller range of operation for the same transmitter power, since the signal has to travel roughly twice the amount of distance as in point-to-point communica-

tion (in mono-static topology), which translates to four times the attenuation (see Friis (1946)).

- Signal impairments unique to backscatter communication, discussed later in section 1.6.

When considering communication applications, the ultra-low power consumption appeals to sensor data communication. With the advancement in fabrication, sensors have become increasingly smaller and consume less energy (see Garfinkel and Rosenberg (2006)).

This work considers the use of backscatter communication for the ultra high frequency (UHF) band spanning 300 Mhz to 3 Ghz, which allows desirable EM propagation for communication purposes. It also has a few bands dedicated to industrial, scientific and medical (ISM) applications which allow easy experimenting and deployment.

1.6 Signal Impairments of Backscatter Communication

- Usually in point-to-point communication, the carrier and the modulation signal are phase synchronized, so at the receiver, estimation of the carrier phase also serves to estimate the symbols phase. This is not the case in backscatter communication as the carrier phase depends on the parameters exogenous to the RF tag, and will require two step phase estimation process.

- Clutter is a unique phenomenon of backscatter communication caused by the EM source reflections not scattered off the tag. This is discussed and analyzed in chapters 2 and 4.

- Multipath looks different than multipath of point-to-point communication. This is discussed and analyzed in chapter 2.

2

Communication Processing

2.1 CW signal processing overview

We would now turn into the logical description of a one-way backscatter communication system based on continuous-wave (CW). The system is comprised of a central base station in mono-static topology and a single RF backscatter tag (multiple tags analysis will be discussed in section 2.6). The goal of the system is to provide a reliable communication method minimizing energy consumption at the RF tag side by using backscatter reflection. The system is assumed to be stationary but the exact relative location of the RF tag is unknown to the reader. The reader transmits constantly a perfect tone consisting of a single frequency or a sinusoid waveform, hence continuous wave. While the CW is transmitted, the reader maintains an on-line communication link, and can potentially receive all signaled data from the tag. The received signal at the reader will contain the reflected CW tone attenuated and modulated with the RF tag modulation signal. Attenuation is a function of the distance propagated (see equation (1.1)). The phase of the reflected CW will be depending on the distance the wave propagated (see Griffiths and College (1999)) and will manifest

as a constant phase difference between the transmitted and received CW, as long as the system is mechanically static. The signal will therefore look very similar to a received signal in a point-to-point communication system, where the carrier signal is replaced with a backscattered CW.

Processing of the received signal is very similar to that of a receiver in point-to-point communication. The receiver starts with recovering the carrier phase using some algorithm (see Johnson and Sethares (2004)), this will ensure that no residues of phase are left after de-mixing with the heterodyne receiver. After using the heterodyne, the signaled data symbols of interest are available. After filtering around baseband to get rid of out-of-band noise and second harmonics, the signal passes through symbols' match filter to optimally detect symbols in white noise (see Lathi (1998)). The next step is not used in point-to-point communication (as tracking the phase of the carrier already gives the phase of the symbols) and it is estimating and tracking the phase of the tag symbols in order to sample them correctly at the symbols center. Various algorithms can be used for that (see Johnson and Sethares (2004)). Then the matched filter output is sampled and passed through a threshold to determine the associated bits.

2.2 FMCW signal processing overview

The use of other type of waveform for backscatter communication, and especially wideband waveforms was suggested in recent research work (see Carlowitz et al. (2013) and Cnaan-On et al. (2014)). In this framework the reader transmits a linear frequency-modulated (LFM) continuous-wave (FMCW), which is a type of waveform widely used for radar and sensing (see Richards (2005)), also sometimes called 'chirp' and see Fig. 2.1. The transmitted signal consists of a train of back-to-back pulses which each is a linear sweep in frequency with constant amplitude. The rate of the pulses is called the 'Pulse Repetition Frequency' (PRF). The sweeps are cen-

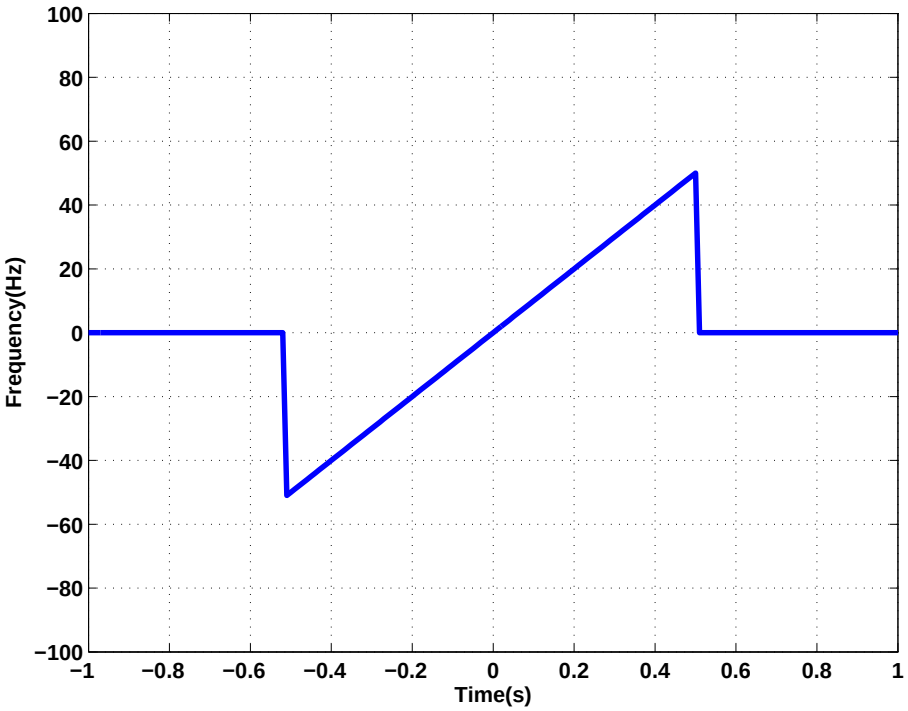


FIGURE 2.1: The LFM waveform envelope with pulse duration $T = 1\ s$ and bandwidth $B = 100\ Hz$

tered around some carrier frequency and span the bandwidth of the start and stop frequency. The sweep can be increasing or decreasing in frequency.

The received signal at the reader will contain the reflected FMCW signal modulated with the RF tag modulation signal. The reflected FMCW will be attenuated and delayed in time because of propagating twice the distance from reader to the tag. For the case when the time delay is shorter than the pulse duration, the receiver will start receiving the backscattered pulse while still transmitting the end of the same pulse. Comparing in real-time the transmitted and the received pulse will demonstrate that the time delay will manifest as a constant frequency difference between the transmitted and received signal, as long as the system is static (see equation 2.8). Processing of the received signal is somewhat analogous to the heterodyne receiver. First the received signal is de-mixed ('de-chirped') by mixing it with the currently transmitted (and conjugated) pulse. The output for that processing is a single tone

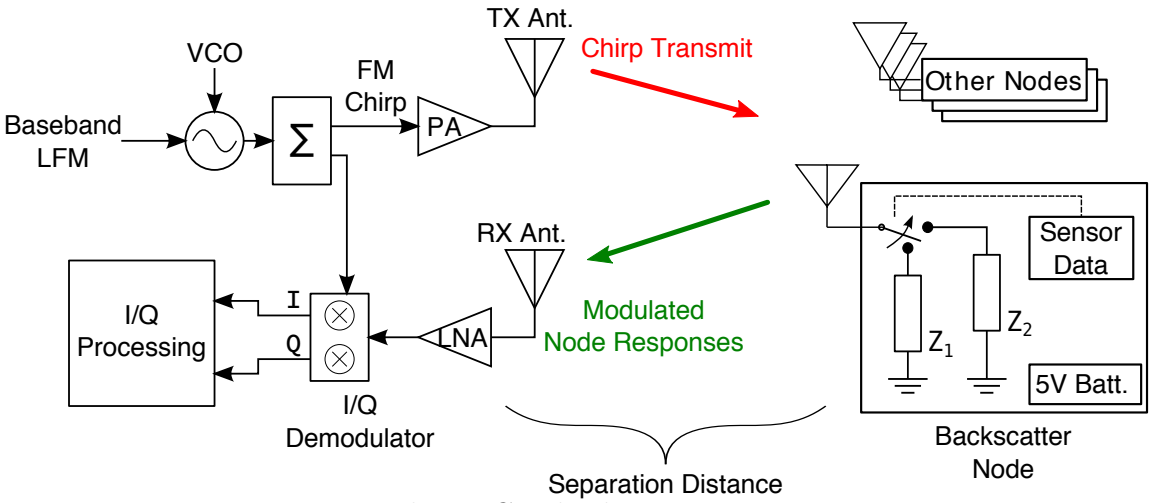


FIGURE 2.2: Example FMCW backscatter communication system

corresponding to the frequency difference between the transmitted and received signal (hence 'range dependent carrier'), modulated by the tag modulating signal. The next step is estimating the frequency and phase of the range dependent carrier using some algorithm (see Johnson and Sethares (2004)), this will ensure that no residues of constant or time-varying phase are left after de-mixing with the heterodyne receiver. The next steps are similar to those described earlier in CW.

When dealing with CW it is assumed to be narrowband signal, which means the bandwidth of the modulated signal does not exceed the channel's coherence bandwidth (where the channel frequency response is considered flat). This is not naturally the case in FMCW, as the bandwidth used can exceeds the channel coherence bandwidth. The more bandwidth is assigned to the FMCW signal, the more distortion the FMCW signal will suffer propagating through the channel. This effect therefore needs to be considered in design and analysis of FMCW commutation system.

A diagram showing backscatter communication for data uplink from sensors interrogated by a radar from some standoff distance is shown in Fig. 2.2. In this scenario, a number of sensors are dispersed in an environment surveilled by a radar.

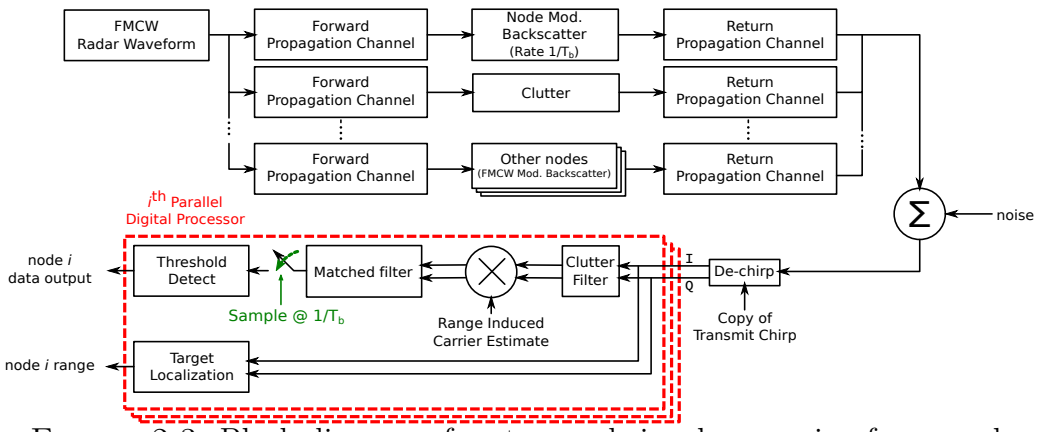


FIGURE 2.3: Block diagram of system and signal processing framework

2.2.1 Comparison of Processing of FMCW and CW

A few differences between CW and FMCW are worth highlighting:

- The time delay of the received CW manifests as a constant phase shift from the transmitted CW. In FMCW it manifests as a shift in frequency and phase from the transmitted FMCW. This makes the FMCW receiver processing more complicated.

- CW requires only a single heterodyne (frequency mixing) operation, while FMCW requires two step of frequency mixing: de-mixing of the FM pulse modulation and de-mixing of the range dependent carrier.

- In CW, tag could utilize the entire time to communicate regardless of the CW phase. In FMCW however, the 'edges' of the chirp pulses can not necessarily be utilized for tag communication. The de-mixing of the FM modulation will mix at the beginning and the end of each a pulse a duration equivalent to the time delay of the tag, where a received pulse is de-mixed with a neighboring pulse (either before or after). See further discussion in section 2.2.3.

2.2.2 FMCW as a Spread-Spectrum

By definition, spread-spectrum is a technique which takes a signal with some bandwidth and spread it in the frequency domain, resulting in a signal with wider bandwidth (see Proakis (2000)).

Previous work have addressed the use of spread-spectrum techniques for backscatter communication. Frequency hopping spread spectrum (FHSS) have used a frequency hopping of the CW center frequency according to some pseudo-random order of hopping. It has been shown to mitigate interferences and some multipath fading (see Banerjee et al. (2008)). Other work (see Durgin and Rohatgi (2008)) have used spread-spectrum techniques by encoding the bits of the tag and thus shaping its spectrum. This is also called direct-sequence spread spectrum (DSSS).

The use of FMCW with RF tag can be seen as a spread-spectrum communication technique. In the case where FMCW is used with a tag, an overall spread-spectrum communication is achieved. The spread-spectrum complexity is being implemented in the reader, leaving the RF tag with simple narrowband hardware design.

Spread-spectrum using FMCW have been analyzed before in literature for point-to-point communication. In Springer et al. (2000) the use of chirps is studied and shown to make communication performance better against frequency selective fading. Other work related to Ultra-wideband (see Dardari et al. (2010)), have shown better area coverage, resilience to interferences, high multiple-access capability and ranging resolution. In addition other benefits are hard to detect covert communication and resistance to deliberate jamming (see Proakis (2000)).

2.2.3 FMCW Pulse-to-Pulse Coherence Effect on Receiver Utilization

For a train of increasing sweep (or decreasing sweep), the de-mixing at the receiver will cause the overlapping area at the beginning and at the end of a pulse a discon-

tinuity of frequency jump, equivalent to the FM bandwidth $f_{rng} + B$. The problem effect might be small though, especially for short time delay, where the relative discontinuity duration is negligible; Utilization is $\frac{T_p - 2 \cdot \tau}{T_p}$ where T_p is the radar pulse duration and τ is the time delay. Another perspective would be to measure utilization not in time, but rather in terms of percentage of utilized symbols. In that case it can be shown that increasing ratio of number of symbols per pulse makes symbol utilization higher, as less symbols suffer from the described edge effect phenomenon. Some possible remedies are:

- Utilizing these pulse edges regions is possible, by de-mixning these areas only with an adjusted carrier frequency. This, however, requires estimating of the time delays precisely by the receiver.
- Use some forward error correcting code (FEC) at the tag that will trade communication rate with auto correction of these lost symbols.
- Decrease pulse utilization below 100%, thus earning the beginning overlap if symbols gap is larger than tag time delay. This, however, does not help in increasing the overall time utilization.
- Another approach is to alternate the FM sweep direction every pulse, such that phase is continuous between pulses. De-mixing will cause the overlapping area at the beginning and end of a pulse to have a different carrier frequency, which is the negative of the range dependent frequency. The receiver in this case will face similar processing challenge.

2.3 Signal Model of Backscatter Communication with FMCW

A block diagram of the proposed system is shown in Fig. 2.3. In this system, the radar transmits a continuous stream of linear FMCW 'chirps' $x(t)$. The sweep rate

$\beta = B/T_p$, where B is the chirp bandwidth and T_p is the chirp duration, determines the instantaneous bandwidth of the signal and is measured in units of Hz/s. A single chirp is described as

$$x_p(t) = e^{j2\pi f_c t + j\pi\beta t^2} \cdot \text{rect}\left[\frac{t}{T_p}\right] \tag{2.1}$$

where f_c is the center carrier frequency and rect$[t]$ is the rectangle function over $[-\frac{1}{2}, \frac{1}{2}]$. The LFM waveform is then

$$x(t) = \sum_{n=-\infty}^{\infty} x_p\left(t - nT_p\right). \tag{2.2}$$

The backscatter modulator in the sensor node is modeled as a single switch that modulates the radar cross section (RCS) of an antenna between a number of values to generate binary coded data (see Hansen (1989); Nikitin et al. (2007) and Thomas et al. (2012)). This system model only considers semi-passive, or battery-assisted passive, sensor nodes which use an onboard battery to supply DC power to the sensor node electronics.

In the most basic implementation, the backscatter modulator switches between two antenna loads with different impedances, i.e., open circuit ($\Gamma = +1$) and short circuit ($\Gamma = -1$), corresponding to two constellation symbol states in a binary phase-shift keying (BPSK) constellation. This modulation can also be viewed as amplitude-shift keying (ASK) with two amplitude levels. Other PSK constellations are possible and have been introduced in Thomas et al. (2012). A portion of the incident wave at the antenna is reflected by the switched load due to the load impedance mismatch and is re-radiated back to the radar (see Green (1963); Hansen (1989)). The switch operates at the symbol rate, not the carrier frequency, so the switching transistors need not be biased for gain at the RF carrier frequency. This minimizes power consumption in the modulator (see Curty et al. (2007); Thomas et al. (2012)). The

message signal driving the node switch is expressed as a series of symbols

$$m(t) = \sum_{k=-\infty}^{\infty} a_k \cdot p\left(t - kT_b\right) \tag{2.3}$$

where $a_k \in \{+1, -1\}$ is the binary phase shift for symbol k and $p(t)$ is a rectangular pulse of the symbol duration T_b representing a single symbol period. When using bigger constellations of PSK, a_k will take other values of phase shift. For example in Quadrature Amplitude Shift Keying (QPSK) $a_k = \{e^{(2n-1)\frac{j\pi}{4}}\}, n = 0, 1, 2, 3$.

The EM fields backscattered from node i are received at the radar with a time delay $\tau_i = 2 \cdot r_i/c$ where c is the speed of light and r_i is the range between node i and the radar.

This work assumes that the node is either stationary, or moving slowly such that the Doppler frequency shift is negligible within a single symbol period. The resulting signal from node i received at the radar is

$$s(t,r_i) = \alpha(r_i)\cdot \sum_{n=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} \Big[\overbrace{x_p(t - nT_p - \tau_i)}^{\text{chirps sent by radar}} \cdot \overbrace{a_k p(t - kT_b - \frac{\tau_i}{2} - \delta_i)}^{\text{backscattered symbols}}\Big] \tag{2.4}$$

where $\alpha(r_i)$ is the attenuation due to the two-way backscatter path of length $2 \cdot r_i$ and δ_i is the delay between the radar clock and the node's clock.

The observed signal at the radar receiver also includes radar clutter as well as multipath reflections of the backscattered signal (see detailed discussion in section 2.5.1). Radar clutter results from reflections of the transmitted chirp signal from stationary elements in the surroundings (such as terrain features, walls, buildings, etc.). The clutter can be modeled as a collection of point scatterers at different ranges, so the cumulative clutter return at the radar is

$$c(t) = \sum_{n=-\infty}^{\infty} \sum_{c \in C} \alpha(r_c) x_p(t - nT_p - \tau_c) \tag{2.5}$$

with C representing the set of clutter points and $\tau_c = 2r_c/c$ is the time delay associated with the range r_c of a clutter point from the radar.

Other nodes are assumed to be operating simultaneously at different ranges $\overline{r} = [r_1, .., r_G]$

$$S(t, \overline{r}) = \sum_{g \in G} s(t, r_g) \tag{2.6}$$

where G is the set of all transmitting nodes and $s(t, r_g)$ is the received signal from a node residing at range r_g as described by equation (2.4).

The total energy at the radar receiver's input port is therefore assumed to be the sum of all the aforementioned signals (see equations (2.4), (2.5) and (2.6)) with additive white Gaussian noise (AWGN) $n(t)$, resulting in

$$\begin{aligned} r(t) &= s(t, r_i) + c(t) + \sum_{g \in G} s(t, r_g) + n(t) \\ &= \sum_{i \in G} \alpha(r_i) \sum_{n=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} \Bigg[x_p \left(t - nT_p - \tau_i\right) \\ &\quad \cdot a_{k,i} \cdot p \left(t - kT_b - \frac{\tau_i}{2} - \delta_i\right) \Bigg] \\ &\quad + \sum_{n=-\infty}^{\infty} \sum_{c \in C} \alpha(r_c) x_p \left(t - nT_p - \tau_c\right) + n(t) \end{aligned} \tag{2.7}$$

where $a_{k,i}$ is the phase shift for symbol k of node i. Multipath reflections of the backscatter signal create copies of $s(t, r_i)$ at multiple ranges resulting from the path taken between the radar and node.

2.4 Receiver Processing of Backscatter Communication with FMCW

Processing the backscattered signal from the sensor nodes includes three steps. First, a de-chirp process akin to range processing is employed to remove the FMCW modulation and obtain a baseband spectrum containing range-dependent subcarriers

for each sensor node. Second, coherent demodulation using an estimated range to the sensor node is employed to demodulate the range-dependent subcarrier. Third, matched filter is employed to recover the sensor data stream.

2.4.1 De-chirp Process (De-mix of radar pulse)

To extract the sensor node uplink data, the first step is similar to range processing where de-chirping via a cross-correlation between the received and transmitted signal is performed. Given a backscatter return from node i at some time delay τ_i, the de-chirp processing yields a corresponding baseband tone whose frequency f_i is a function of the time delay $f(\tau_i)$. Thus, the received data uplink is

$$r_d(t) = \alpha(r_i) \sum_{n=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} \Big[\overbrace{a_k p(t - kT_b - \frac{\tau_i}{2} - \delta_i)}^{\text{node symbols}} \cdot \overbrace{e^{j2\pi\beta\tau_i(t-nT_p)}}^{\text{range induced subcarrier}}\Big]. \tag{2.8}$$

2.4.2 Demodulating the Range Induced Carrier

The second step is to demodulate each sensor node uplink from the composite received spectrum and to extract its individual spectrum. Given an initial estimate of the node range (either from previous knowledge about the relative range of the tag from the reader or by estimating the range using ranging techniques, see chapter 3), the corresponding subcarrier frequency f_i is estimated and used to demodulate the communications signal. The conjugated carrier replica is $e^{-j2\pi\beta\tau_q t}$ such that $\tau_q = \tau_i$. This carrier replica is mixed with the de-chirped signal. The mixing products are low pass filtered with a cut off at $|f| \leqslant \frac{1}{T_b}$ to recover the baseband signal originating

from the i-th node.

$$\begin{aligned} r_b(t) = r_d(t) \cdot e^{-j2\pi\beta\tau_q(t-nT_p)} &= \alpha(r_i) \sum_{n=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} \\ & a_k p(t - kT_b - \frac{\tau_i}{2} - \delta_i) \cdot e^{j2\pi\beta(\tau_i-\tau_q)(t-nT_p)} \\ & \underbrace{=}_{\tau_q=\tau_i} \alpha(r_i) \sum_{k=-\infty}^{\infty} a_k p(t - kT_b - \frac{\tau_i}{2} - \delta_i) \end{aligned} \tag{2.9}$$

Range estimation error in the demodulation process has a similar impact as carrier frequency uncertainty in conventional systems (see Franks (1980)).

2.4.3 Matched Filtering to Recover Node Symbols

After removal of the range induced carrier, the baseband symbols are recovered via matched filtering with an output $r_{\mathrm{MF}}(t)$ where

$$\begin{aligned} r_{\mathrm{MF}}(t) &= \int r_b(t-u) p^*(-u)\,\mathrm{d}u \\ &= \alpha(r_i) \sum_{k=-\infty}^{\infty} a_k \\ &\quad \int p\big(t - kT_b - \frac{\tau_i}{2} - \delta_i - u\big) p^*\big(-u\big)\,\mathrm{d}u \\ &= \alpha(r_i) \sum_{k=-\infty}^{\infty} a_k \,\mathrm{tri}\left(t - kT_b - \frac{\tau_i}{2}\right) \end{aligned} \tag{2.10}$$

where $p(t)$ is a rectangular pulse, and $\mathrm{tri}(\cdot)$ is the triangle function. The phase offset δ_i between the radar and the node can be estimated from a training preamble; a variety of well known methods for estimating this offset may be applied (see Franks (1980)). After standard sampling and thresholding of the matched filter output, the data bits of the tag can be recovered.

2.5 Coding Utilization for Clutter Filtering with FMCW

The following section discusses clutter when using CW or FMCW waveforms. Clutter is modelled as static returns and two clutter mitigations algorithms are discussed. Further discussion on spread Doppler clutter model and generalized waveform can be found in chapter 4.

2.5.1 Clutter Reflections Model in CW and FMCW

In any backscatter communication the EM source emits waveforms which not all are scattered from the RF tag. Some are being reflected from other objects in the surroundings such as ground, walls, ceiling and other objects. These reflections are called 'clutter' in radar jargon. Some reflections can scatter more than once before reaching the receiver. These static reflections or 'clutter' returns can be viewed or modeled as a collection of point scatterers that comprise all non tag related reflections being received by the receiver. Generally, the amount of clutter reflections energy depends on the proximity, density and material of reflecting objects in the environment. For example, indoor environment produce a lot of clutter reflections, while outdoor usually has lower levels of clutter reflections. High levels of clutter, similar to noise, will obscure the signal of interest. One metric for that is the signal to clutter plus noise power ratio (SCNR), which resembles the signal to noise power ratio (SNR). Some simple methods of clutter filtering are to use directional transmit and/or receive antennas or to use phased antenna array processing to minimize scattering from clutter points. Statistically, clutter is uncorrelated with the RF tag symbols, but highly correlated with the EM source.

When CW is used, each clutter reflecting point will be received by the receiver as an a attenuated version of the transmitted CW with phase constant phase shift from

the transmitted CW. The attenuation and phase shift are functions of the distance traveled before arriving at the receiver (see equation (1.1) and Griffiths and College (1999)). After heterodyne de-mixing, each clutter point will effectively produce a constant phase added to the receiver output, and when added all together it yields the 'clutter profile' of that specific environment.

When FMCW is used, each such reflecting point will be received by the receiver as an a attenuated and time delayed version of the transmitted signal. The attenuation and time delay are functions of the distance traveled before arriving at the receiver (see equation (1.1) and Griffiths and College (1999)). After de-mixing with the transmitted FMCW signal, each clutter point will effectively produce a tone with frequency and phase, corresponding to that clutter point time delay, that will be added to the receiver output. Thus, clutter from a set of point scatterers will manifest, after processing, as a continuum of uncorrelated sinusoids at the receiver output (de-chirped domain and see subsection 2.4.1), which in the time domain appears noise-like. Assuming the point scatterers are stationary (with zero or near-zero Doppler shift), the output of the de-chirp process due to clutter will be identical from chirp to chirp, acting as a cyclo-stationary process. This can be observed in Fig. 2.4

In CW, which is the dominantly used technique for backscatter communication, the effect of clutter is minimal. As described in section 2.5.1, after heterodyne de-mixing at the receiver, each clutter point will effectively produce a constant phase added to the receiver output, and when added all together it yields the 'clutter profile' of that specific surroundings. Since this addition to the signal of interest from a tag is constant over time, it is possible for the receiver to correct for the constant phase shift by shifting the PSK constellation, which is a common task in communications (see Proakis (2000)). In FMCW, clutter has different effect and handling it needs to be done differently.

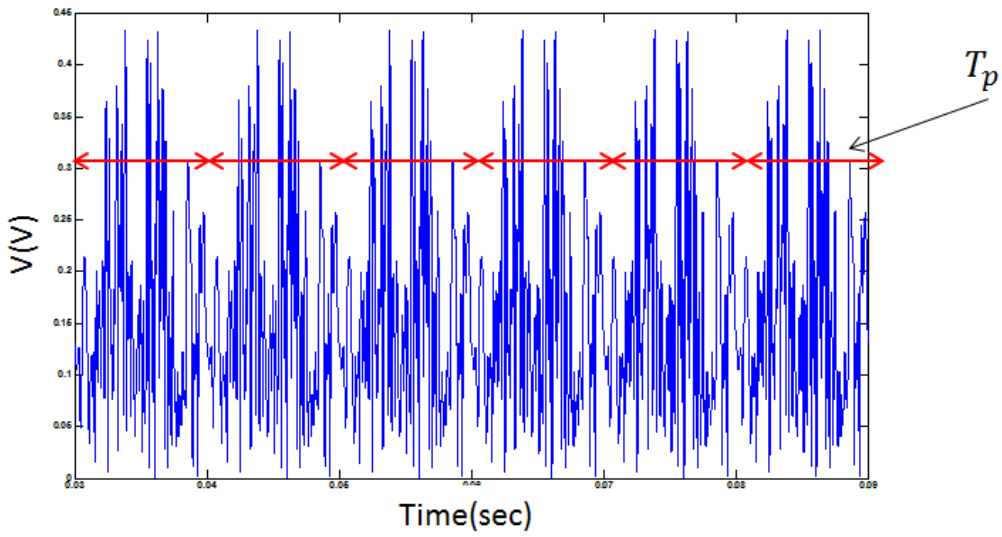
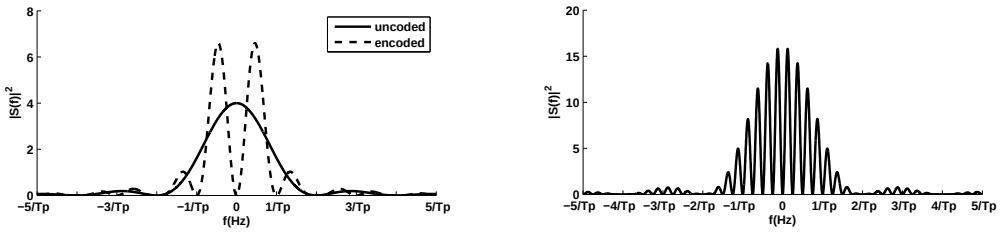


FIGURE 2.4: Simulated clutter return in FMCW system, when observed after de-chirping the radar pulse

2.5.2 Modeling Clutter as Cyclo-Stationary Process in FMCW

In a typical scenario where the spatial density of sensor nodes is low, the total amount of clutter energy will far exceed the amount of energy backscattered from nodes. Clutter from a set of point scatterers manifests as a continuum of uncorrelated sinusoids in the de-chirped baseband spectrum, which in the time domain appears noise-like (and see section 2.5.1). However, assuming the point scatterers are stationary (with zero or near-zero Doppler shift), the output of the de-chirp process due to clutter will be identical from chirp to chirp, acting as a cyclo-stationary process. Leveraging this observation, moving target indication (MTI) processing was developed for rejecting stationary clutter (see Richards (2005)). In the simplest MTI implementation, the de-chirped baseband return profile of chirp $(n-1)$ is subtracted from chirp n. Stationary clutter, which is identical from chirp to chirp, is thus rejected.

It is worth noting that under realistic conditions, as the radar pulse duration T_p



(a) (b)

FIGURE 2.5: Simulated baseband spectrum for the line coding of algorithm 1 with (a) $M = 2$ and no coding for comparison, and (b) $M = 8$

increases, clutter returns from consecutive pulses may no longer be assumed to be identical. From a practical perspective, it is therefore beneficial to opt for a shorter radar pulse duration as MTI clutter mitigation is more robust.

2.5.3 Algorithm 1, Line-Coding Across Exact Neighboring Chirps

The clutter suppression of MTI processing is leveraged to implement a simple line coding technique that allows the desired node uplink signal to be separated from the stationary clutter. In this technique, the node transmits a set of symbols corresponding to a desired message block of length M (the number of symbols per chirp duration) which occupies the entire duration of the chirp over e.g., $0 < t \leqslant T_p$. On the following chirp duration (e.g., $T_p < t \leqslant 2 \cdot T_p$), the node transmits a negated version of the same set of symbols, such that $a_k = -a_{k+M}$. This coding then continues for the next pair of chirp pulses. The radar receiver decodes each pair of received baseband series by subtracting the second from the first. Stationary clutter is thus removed (as in standard MTI processing) while the decoded symbols are now enhanced as they have twice unit energy. For example, consider a trivial case of sending a message comprised of 4 symbols with this method:

$$\overbrace{(-1+1-1-1)}^{\text{first chirp}} - \overbrace{(+1-1+1+1)}^{\text{second chirp}} \Longrightarrow \overbrace{(-2+2-2-2)}^{\text{decoded}}$$

More formally, the decoding is performed on the received node signal-plus-clutter

after the de-chirp process (see section 2.4.1) and before demodulation with the range induced carrier 2.4.2:

$$r_d(t) = \sum_n \Bigg(\alpha(r_i) \sum_{k=-\infty}^{\infty} \Big[a_k p(t - kT_b - \frac{\tau_i}{2} - \delta_i) \cdot e^{j2\pi\beta\tau_i(t-nT_p)} \Big] + \sum_{c \in C} \alpha(r_c) e^{j2\pi\beta\tau_c(t-nT_p)} \Bigg) \tag{2.11}$$

This approach is a chirp-to-chirp coherent subtraction by processing chirp pairs yielding

$$r_{\text{decode}}(t) = \sum_{\text{odd } n} \left(\alpha(r_i) \sum_{k=-\infty}^{\infty} \Big[2a_k p(t - kT_b - \frac{\tau_i}{2} - \delta_i) \Big] \cdot e^{j2\pi\beta\tau_i(t-nT_p)} \right) \tag{2.12}$$

This line-coding approach results in each symbol of the message having twice the unit energy, while stationary clutter drops out. A simulated baseband spectrum showing this effect for message lengths $M = 2$ and $M = 8$ is provided in Fig. 2.5.

In this coding method the RF tag must be synchronized with the pulse repetition frequency (PRF) phase of the FMCW signal in order for the coding to be exactly inverting the bits on a neighboring chirp. This requirement will require an additional hardware to handle the synchronization and will be costly in terms of energy. Therefore the developed algorithm 2 can relax the requirement for synchronization by using differential instead of relative encoding.

2.5.4 Algorithm 2, Differential Line-Coding

Differential line-coding uses similarly to the relative line-coding, the fact that the clutter can be modeled as a cyclo-stationary process. Instead of coding the bits relatively to their location in a chirp, they will be now encoded differentially with the chirp duration separation. This will not require a synchronization or estimation

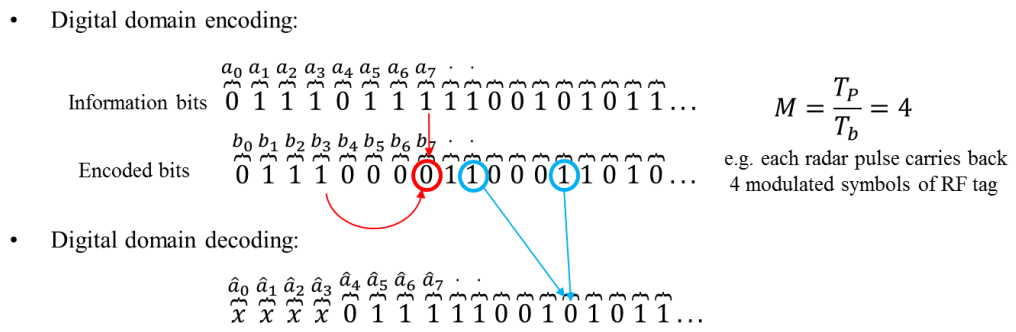


FIGURE 2.6: Differeential Line-coding technique for clutter mitigation

with the PRF phase, but will require the PRF rate. In a system where the PRF is a design parameter, this value should be available also for the tags in their set-up process. The algorithm in the bit domain uses Exclusive OR (XOR) operation for bits encoding and decoding. See Fig 2.6.

$$\text{Encoding: } b_n = b_{n-M} \oplus a_n \tag{2.13}$$

$$\text{Decoding: } \hat{a}_n = b_{n-M} \oplus b_n \tag{2.14}$$

$$\tag{2.15}$$

where a_n is bit n of the data to be signaled, b_n is bit n of the decoded data, M is the number of symbols per radar pulse and $\hat{a}_n$ is the n^{th} bit of the recovered data

However, the clutter filtering and line-decoding is performed in the analog domain. There, the signals subtraction creates 3 levels of voltage ($(+1)-(-1) = +2, (-1)-(+1) = -2, (+1)-(+1) = 0$ or $(-1)-(-1) = 0$) rather than 2 (see Fig. 2.7). The result maintains same SNR as uncoded signal as the increase in gap between levels is offset by the increase of number of decision regions.

2.6 Backscatter Communication Multiple Access and Collision Avoidance

In many scenarios, it is required that more than a single RF tag will be operating in a given interrogation zone. For the common case that CW or FMCW is used,

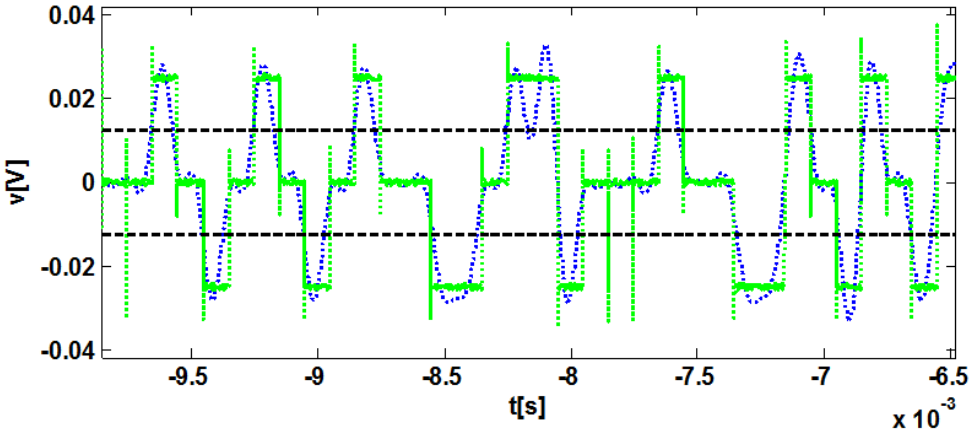


FIGURE 2.7: Simulation and analyical results of decoded signal using differential Line-coding. Decision region boundaries are marked as dashed lines.

all of these tags will be backscattering simultaneously towards the reader. From the perspective of the reader, collisions of multiple tags occurs when two tags backscatter on the same time, causing cross interference and in many cases inability of the reader to separate between tags data streams. Throughput of tags reading has been shown to reduce rapidly when the number of tags inside an interrogation zone is increased (see Su et al. (2010)).

Literature have also addressed the case when multiple readers interrogate simultaneously a given zone. For example Mohsenian-Rad et al. (2009) explores such sharing algorithm. This work, due to space limitations, does not address the case of more than one reader.

Collision avoidance or collision recovery are active research areas addressing this issue. The work in Wang et al. (2012) developed a method of seeing RF tags collision as a code and decoding is being done using compressive sensing algorithm. The work in Angerer et al. (2010) demonstrate a method of recovering data from a collision on the physical layer, by separating tags signals on the I/Q (In-phase/quadrature) plane and also spatially by using multiple reader antennas. The work in La Porta

et al. (2011) analyzes a Media-Access Control (MAC) layer algorithm based on tree structure and on the commonly used ALOHA algorithm. It is worth mentioning here that the anti-collision algorithm used in the EPCglobal Gen2 standard used for many RFID applications, is the framed slotted ALOHA (FSA) based on discrete time-slots assignment (see EPC Global US (2005)).

2.6.1 Multiple Access with FMCW

As described in section 2.3, the sensor node's data stream appears in the de-chirped baseband as double-sideband amplitude shift keying (ASK) or phase shift keying (PSK) modulation of a subcarrier corresponding to the distance from the radar to the node. Therefore, the signal from the i-th node is centered around f_i as shown in the spectrum of Fig. 2.8. In this figure, the node transmits at symbol rate $1/T_b$ which sets the occupied bandwidth. The subcarrier and occupied bandwidth of a single RF tag can be viewed as a channel in the frequency domain. Multiple tags at other ranges will result at many such channels that can operate simultaneously.

The backscattered signal from the nodes can be generally described as an infinite train of random symbols with a binary ASK or binary PSK modulation. The simple binary-switch modulator initially shown in Fig. 2.2 produces unshaped, rectangular symbols due to the near-instantaneous switching of the antenna between two load impedances. Fourier analysis of these signals (see Stern and Mahmoud (2003)) yields a closed form derivation of the averaged spectrum

$$G(f) = A^2 T_b \operatorname{sinc}^2(\pi f T_b) \tag{2.16}$$

where A is the pulse amplitude and T_b is the symbol duration. Approximately 90% of the signal energy is concentrated in the $\pm\frac{1}{T_b}$ range around the node's subcarrier frequency. The amount of upper-sideband energy in the range of $\frac{1}{T_b} \leqslant f \leqslant \frac{2}{T_b}$ (or equivalently in the lower sideband $-\frac{2}{T_b} \leqslant f \leqslant -\frac{1}{T_b}$) is only $\approx 2.5\%$, or -16 dB

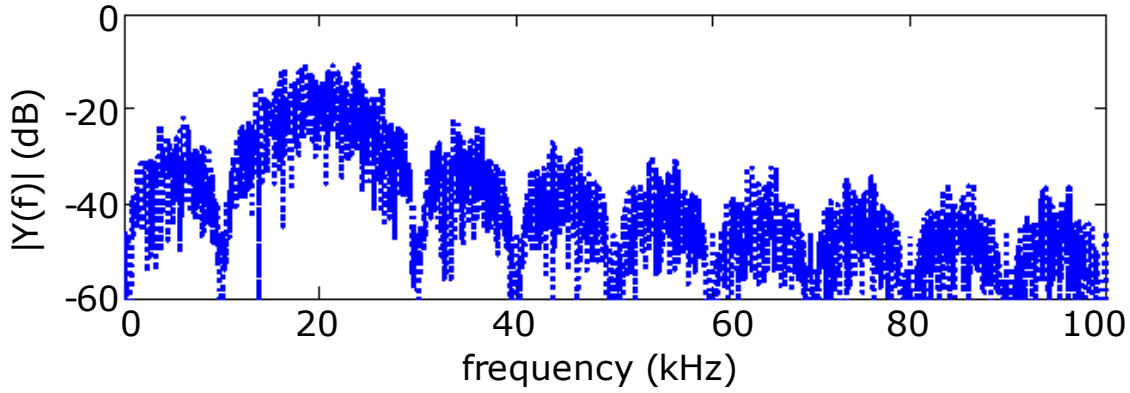


FIGURE 2.8: Simulated received power spectrum of node transmitting at rate $1/T_b$ = 10 kHz at range of 15 m corresponding to a range subcarrier of 20 kHz

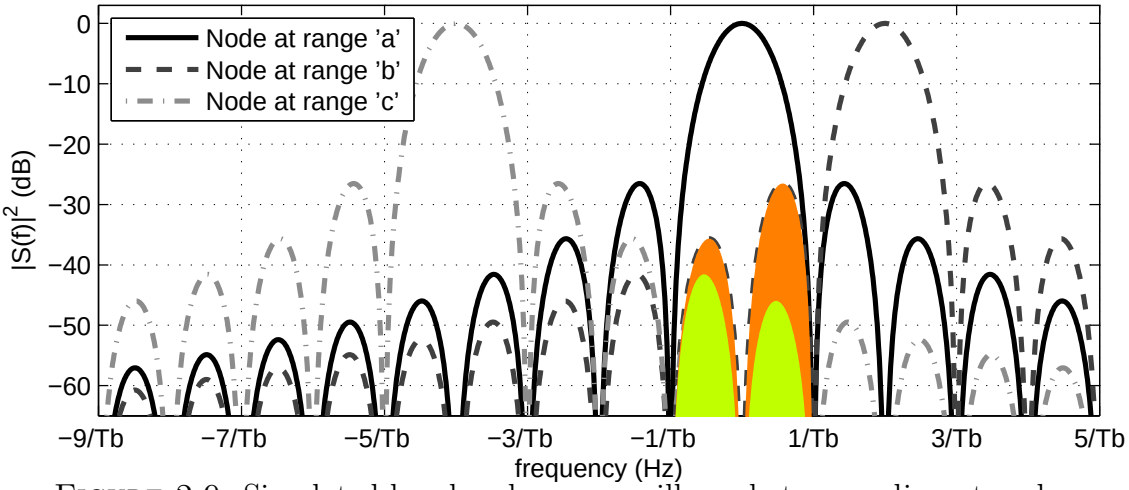


FIGURE 2.9: Simulated baseband energy spillover between adjacent nodes

relative to the in-band energy. In the case of two neighboring nodes, separated exactly by the range bound and transmitting at the same rate, the adjacent channel energy in the nearest neighbor's channel is suppressed by the same 16 dB. Figure 2.9 illustrates this spillover between adjacent nodes. Nodes 'a' and 'b' are separated exactly by the range bound while nodes 'a' and 'c' are spaced farther apart in range. The shaded areas represent the energy spillover into node 'a' baseband spectrum.

2.6.2 Upper Bound on Node Spatial Density and Node Data Rate using FMCW

The minimum spacing (in range) for nodes that avoids aliasing in the de-chirped baseband during simultaneous transmission is considered. We assume nodes are spaced in range by $\Delta r_{\min}$. The respective frequency spacing between range-induced subcarrier frequencies is then

$$f_1 - f_2 = \Delta f_r = \beta \Delta \tau = \frac{B}{T_p} \frac{2\Delta r_{\min}}{c} \tag{2.17}$$

Assuming node 1 transmits at symbol rate $1/T_{b_1}$ while node 2 transmits at symbol rate $1/T_{b_2}$, to prevent spectral overlap between the two nodes the system must satisfy

$$\frac{B}{T_p} \frac{2\Delta r_{\min}}{c} \geqslant \left[\frac{1}{T_{b_1}} + \frac{1}{T_{b_2}} \right] \tag{2.18}$$

This bound provides a fundamental trade-off between node data rate, node range separation and the bandwidth of the LFM radar waveform. In other words, uplink rate is bounded by the range difference between simultaneously transmitting nodes. Also, as the bandwidth of the LFM radar waveform is increased, the symbol rate at which the nodes can transmit without causing spectral overlap with neighboring nodes also increases.

2.7 Multipath Propagation Analysis in CW and FMCW

Multipath propagation happens when the backscattered RF tag signal reach the receiver by more than one propagation path as a result of reflection from an intermediate object. The resulting received signal is an overlap of all multi-path signal copies, each with other delay corresponding to the path traveled. The shortest possible path is called 'line-of-sight' (LOS) and it refers to EM traveling in straight line from the EM source to the RF tag and backscattered back towards the receiver in a straight line as well. Geometrically, using the triangle inequality, it can be argued

that when a line of sight exists (such that EM can travel in a direct path without any blockage), it will be with the shortest delay of all other multipath and its delay will corresponds directly with the actual distance between the tag and the EM source. Multipath reflections are highly correlated with both the transmitted EM signal and the tag modulation signal.

When CW is used, multipath would appear at the input of the receiver as a sum of different delayed signals of the CW modulated with the tag modulation signal. After de-mixing with the transmitted CW, the signal will contain a summation of the tag modulating signal delayed and residue of constant phase contributed from the delayed CW de-mixing (same delay as the tag modulating signal). At this point the multipath will become what is known in point-to-point communication as the Inter-symbol interference (ISI), which would look as duplicate delayed copies of each symbol corresponding to each multipath, see the 'eye diagram' which visually measure that in Fig. 2.10. The amount of ISI will determine the ability of the receiver to correctly recover the original modulation signal (see Lathi (1998)). For example in an indoor surroundings, the amount of multipath is high and the original symbol might not be recoverable as is. Methods of equalization (see Proakis (2000)) or channel estimation would be able to minimize the ISI effect (and see Bharadia et al. (2015)).

When FMCW is used, multipath would appear at the input of the receiver as a sum of different delayed signals of the FMCW modulated with the tag modulation signal. After de-mixing with the transmitted FMCW, the signal will contain a summation of the tag modulating signal delayed and mixed with range induced carrier contributed from the delayed FMCW de-mixing (same delay as the tag modulating signal). At this point each multipath will contain the tag modulating signal centered

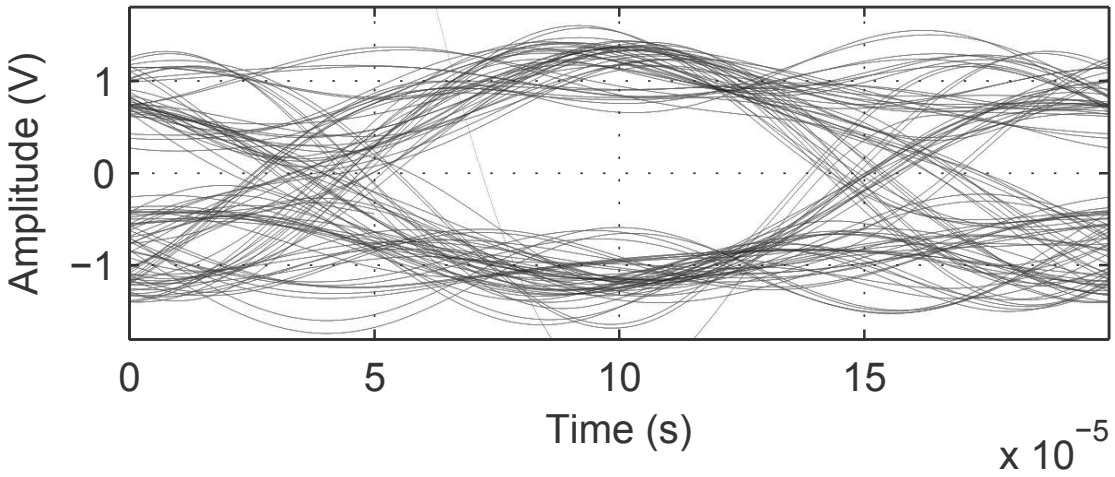


FIGURE 2.10: Measured eye diagram for RF tag backscatter

around a different range induced carrier.

2.7.1 Backscatter Communication Multipath Mitigation Overview

The work in Wang and Katabi (2013) explores the use of Synthetic Aperture Radar (SAR) created via antenna motion to create multipath profile and used Dynamic Time Warping (DTW) to separate between tag neighbors that exhibit similar multipath profile. The work in Lunglmayr and Huemer (2010) proposes a least squares equalization that uses linear method to equalize the channel and utilize the multipath signals to increase overall signal to noise ratio (SNR). The work in Griffin and Durgin (2009b) have provided detailed measurements of multipath fading with various multiple antennas settings. The work in Ingram et al. (2001) have explored a way to reduce multipath fading through antenna diversity which uses multiple antennas at the reader to provide spatially separated diversity. The work in Griffin and Durgin (2008) have explored a way to reduce multipath small-scale fading through antenna diversity which uses multiple antennas at the RF tag to provide spatially separated diversity.

2.7.2 Modeling of Multipath Reflections in FMCW

For a single tag, with some Q multipath reflections of different path lengths $\overline{r} = [r_1, .., r_Q]$

$$S(t, \overline{r}) = \sum_{q \in Q} s(t, r_q) \tag{2.19}$$

where Q is the set of all multipath (including line of sigth (LOS) if exists) and $s(t, r_q)$ is the received signal from a multipath with path length of r_q as described by (2.4).

2.7.3 Use of Spectral Filtering for Partial Mitigation of Multipath in FMCW

As described earlier in section 2.7, in FMCW the multipath causes interference or fading to the received tag signal. After the de-chirp process multipath will manifest as overlap of the modulating signal bandwidth in the frequency domain with other multipath modulating signal bandwidth on another range induced carrier. By filtering around the bandwidth of the desired carrier (as described in section 2.6.1), it is possible to partially filter other multipath signals, but not entirely.

2.8 Experimental Results

To validate this approach, a brass-board bistatic S-band radar and accompanying backscatter sensor nodes were constructed. A block diagram of the system is shown in Fig. 2.3, with the digital processing blocks implementing the algorithms described above. The radar transmits at a center frequency of 2.45 GHz with a bandwidth of 40 MHz and a chirp rate of 5 kHz.

The radar's LFM waveform is generated using an Agilent N4181A RF signal generator utilizing the onboard FM option, modulated by an Agilent 33220A arbitrary waveform generator configured to generate a sawtooth linear ramp at baseband.

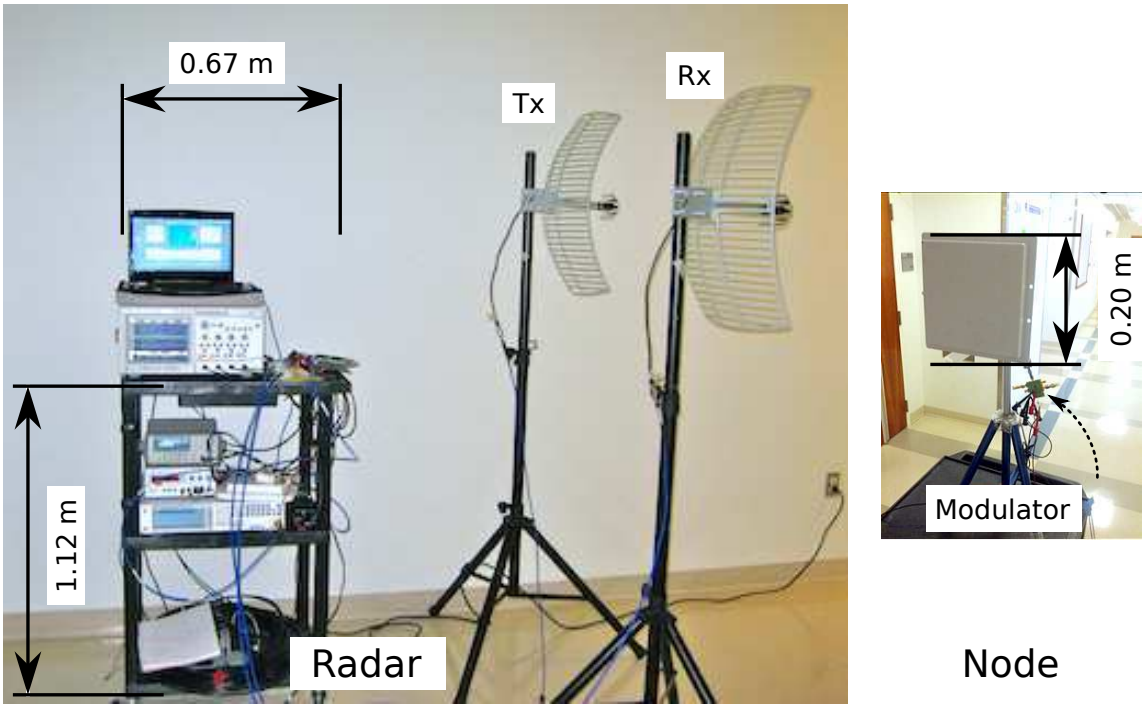


FIGURE 2.11: Photograph of experimental radar setup in 60 m indoor hallway

The LFM signal is amplified using a MiniCircuits ZRL-3500+ power amplifier to a conducted power level of 26 dBm and transmitted through an L-COM HG2420EG antenna with 20 dBi gain and horizontal polarization. A photograph of this setup is shown in Fig. 2.11.

The semi-passive backscatter nodes were realized using a Hittite HMC241LP3 RF switch and an L-COM HG2414P 14 dBi S-Band patch antenna. The baseband data applied to the RF switch is provided by another Agilent 33220A arbitrary waveform generator controlled by a PC running Matlab. This method of data generation was chosen for increased flexibility in testing the communication link. In practice, data would be passed to the modulator using a low-power microprocessor or FPGA.

For the radar's receiver, a second L-COM HG2420EG antenna is used in a bistatic configuration in conjunction with a Mini-Circuits ZRL-3500+ RF amplifier with 20 dB gain and 2.5 dB noise figure. The received signal is de-chirped in hardware, with a copy of the transmitted signal feeding the LO port of a Linear Technologies

LT5575 I/Q demodulator. The de-chirped complex baseband spectrum is passed to an Agilent DSO8104 oscilloscope which is used for data capture. Digital processing is performed in Matlab as outlined in Fig. 2.3.

Operation of the system was first validated and characterized in an anechoic chamber and then in an indoor hallway with a maximum length of approximately 60 m. At this output power, based on the parameters in Table 2.1, a maximum theoretical operating distance of 2 km is expected for the system to yield a SNR of 10 dB corresponding to $\leqslant 10^{-3}$ bit error rate for BPSK signaling from a single node. The differential radar cross-section (DRCS) $\Delta\sigma$ of 4.76 dBsqm was found using the relation

$$\Delta\sigma = \frac{\lambda^2 G_{\text{ant.}}^2}{4\pi}|\rho_1 - \rho_2|^2$$

where $G_{\text{ant.}}$ is the antenna gain (14 dBi), and $\rho_{1,2}$ are the power reflection coefficients (see Nikitin et al. (2007)). In this brass-board, the range limitation is due mainly to the dynamic range of the 8-bit ADCs in the Agilent DSO8104 oscilloscope used for baseband data capture. Another limitation introduced by the use of the oscilloscope is limited baseband sample length; only 8 Mpts of data can be acquired in a single capture. One significant consequence of the limited baseband sample length is the inability to measure long runs of data; thus the BER measurements we present should be considered upper bounds on the true BER.

2.8.1 Single Node In View

Experimental results with a single node uplink at 30 meters in the test hallway are shown in Fig. 2.12. The spectrum of the de-chirped baseband signal is shown in the light trace. The dominant components of the baseband spectrum are the peaks corresponding to stationary clutter in the hallway (multipath along the hallway), due to the periodicity of the clutter signal induced by the repetitive nature of the

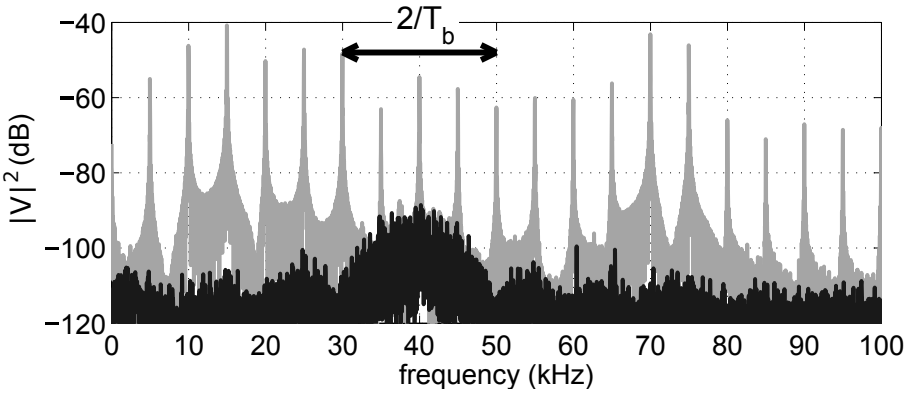


FIGURE 2.12: Measured power spectrum of received signal before (light) and after (dark) clutter filtering with node signal is centered around subcarrier of $f_i = 40$ kHz, parameters used: f_c=2.45 GHz, B=40 MHz, T_p=20 ms, T_b=40 ms

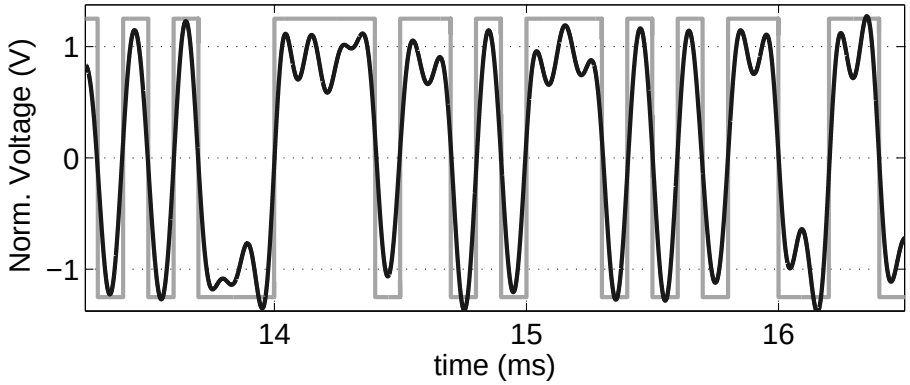


FIGURE 2.13: Measured received signal waveform after removal of range induced carrier and clutter (dark) and transmitted signal waveform (light), parameters identical to Fig. 2.12

radar chirps. The signal of interest (SOI) from the sensor node is masked by the clutter in the de-chirped signal, but can be recovered by differencing chirp pairs as discussed above. The resulting SOI is clearly visible in the dark trace. The time domain digital data recovered after removing the range induced subcarrier is shown in Fig. 2.13. The measured bit error rate (BER) is known to be $< 4 \times 10^{-3}$ (zero errors were observed, but limited oscilloscope sample length prevented measurements below this BER).

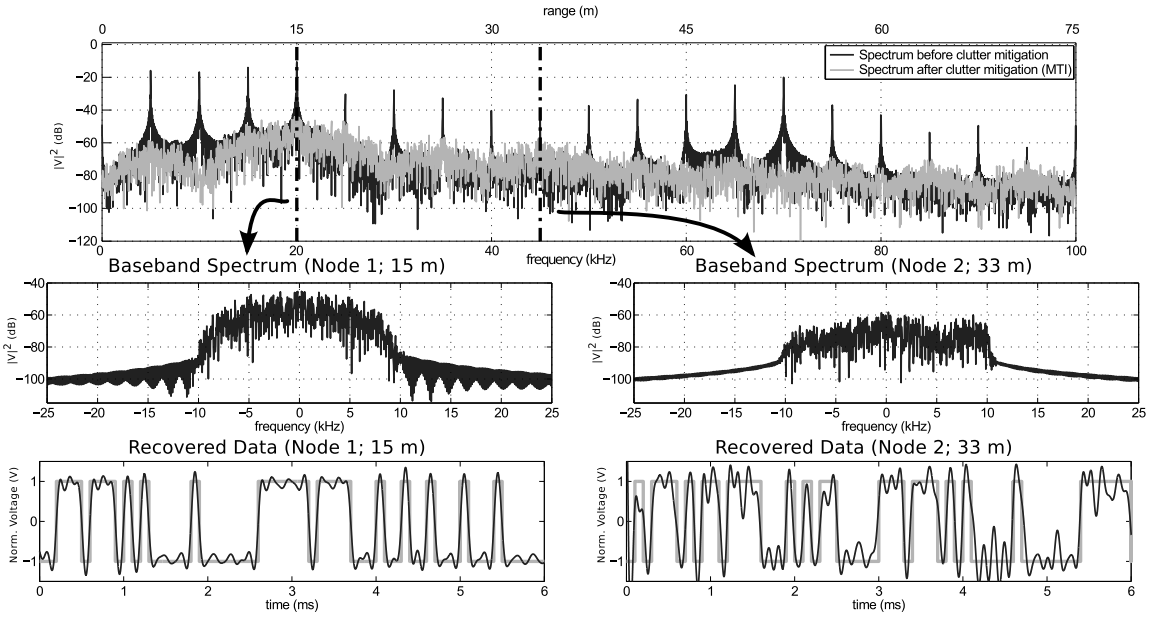
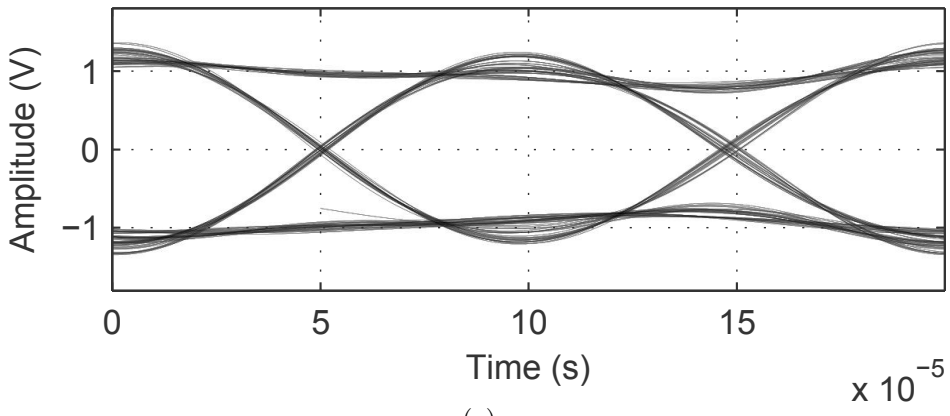


FIGURE 2.14: Measured received power spectrum of two nodes simultaneously transmitting (top), filtered baseband power spectrum of nodes after range separation (middle row) and recovered data waveform versus transmitted signal waveform prior to matched filtering (bottom row)

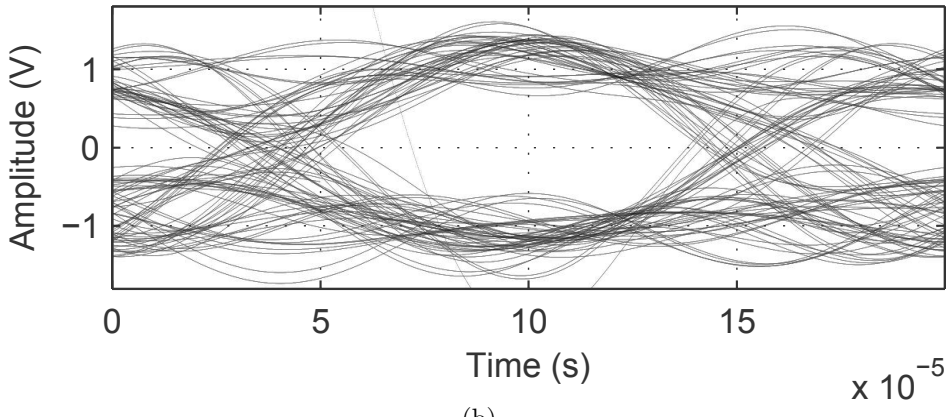
2.8.2 Multiple Nodes in View

Fig. 2.14 presents the result of an experiment demonstrating the recovery of two backscatter nodes in view simultaneously. In this experiment, each node is signaling at a rate of $1/T_b = 10$ kHz and experimental parameters are otherwise similar to previously described experiments (f_c=2.45 GHz, B=40 MHz, $1/T_p$=5 kHz, $1/T_b$=10 kHz).

Since only a single physical node was available for the experiment, the node was positioned at two separate distances and the de-chirped baseband was captured at each distance. The distances of 15 m and 33 m were chosen to satisfy the range bound previously derived for the given data rate. The raw baseband signals were then summed together to generate the test signal. This quasi-realistic model is expected to be representative of the two-node case because the channel is linear and the raw complex baseband signals are added in-phase.



(a)



(b)

FIGURE 2.15: Measured eye diagram for (a) node at 15 m and (b) node at 33 m

The top row of Fig. 2.14 shows the two-tag baseband power spectrum before (dark) and after (lighter) clutter mitigation and demodulation with the range-induced subcarriers for the two nodes (highlighted with dashed lines). Ranges to nodes were found over-the-air by examining the range-Doppler space while nodes transmitted a slow ($1/T_b < 1/T_p$) preamble (01010101 repeated). After clutter mitigation and demodulation with the two range-induced subcarrier replicas, the resulting baseband signal was then filtered using a low-pass filter with a cutoff of $f_{\text{cutoff}} = 1/T_b$ to remove out-of-channel energy. The filtered baseband power spectrum for both tags are shown in the middle row of Fig. 2.14. The time-domain recovered data is shown in

Table 2.1: Example FMCW Backscatter Link Budget

Radar output power	P_t	+26 dBm
Radar antenna gain	G_t, G_r	20 dBi
Carrier wavelength (freespace)	λ	12.2 cm
Node Differential RCS	$\Delta\sigma$	4.76 dBsqm (est.)
Node Bandwidth Limit	BW	100 kHz

the bottom row of Fig. 2.14 in black, overlaid with the transmitted data in gray. Due to the increased range, the signal from the farther node (33 m) suffers from a lower signal-to-noise ratio, but the recovered data still faithfully follows the transmitted signal. This effect can be observed more clearly in the eye diagrams for each node shown in Fig. 2.15. After matched filtering, all bits were compared to the transmitted bits and no bit errors were observed within the limits of the capture buffers (BER $< 4 \times 10^{-3}$).

3

Localization

3.1 Localization Processing with FMCW

The model for the received signal at the receiver input as described earlier in chapter 2 is

$$r(t) = s(t, r_i) + c(t) + \sum_{g \in G} s(t, r_g) + n(t) \tag{3.1}$$

where $s(t, r_i)$ is the backscattered signal from node i, $c(t)$ is the set of clutter points returns, G is the set of all transmitting nodes and $s(t, r_g)$ is the received signal from a node residing at range r_g and $n(t)$ is additive Gaussian white noise.

Range localization of the node is achieved by pulse compression. In this process, the cross-correlation between the received signal $r(t)$ and the transmitted chirp pulse signal $x(t)$ in the time domain is computed (see Richards (2005))

$$r_d(t) = \langle r, x \rangle(t) = \int_{t'=-\infty}^{\infty} r(t') x^*(t + t') dt'. \tag{3.2}$$

This correlation is typically performed as a two-step process: 1) de-chirping or de-ramping, and 2) Fourier transform in fast time. The outcome of the de-chirp process

is

$$r_d(t) = \sum_{i \in G} \alpha(r_i) \sum_{n=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} \overbrace{\Big[\overbrace{a_{k,i} p(t - kT_b - \frac{\tau_i}{2} - \delta_i)}^{\text{backscattered symbols}} \cdot \overbrace{e^{j2\pi\beta\tau_i(t-nT_p)}}^{\text{range induced subcarrier}}\Big]} + \sum_{c \in C} \alpha(r_c) \sum_{n=-\infty}^{\infty} \overbrace{e^{j2\pi\beta\tau_c(t-nT_p)}}^{\text{clutter point-scatterer return}} + \tilde{n}(t) \tag{3.3}$$

where τ_i is node i delay, δ_i is delay between the radar's clock and the node's clock and $\tilde{n}(t)$ is AWGN.

For a return at some time delay τ_i, the de-chirp processing associates a corresponding induced tone whose frequency f_i is a function of that time delay τ_i. The exact range of the node of interest can then be recovered via a discrete Fourier transform and the relation

$$f_i = \beta \cdot \tau_i = \frac{2Br_i}{cT_p} \tag{3.4}$$

In the case of a single scatterer point (such as a clutter point or an inactive sensor node), a single tone will be present in the received signal after pulse compression that corresponds to the time delay. However, in the case of an actively-backscattering sensor node, the signal contribution is a time-domain multiplication of the node signal $m(t)$ and the range induced subcarrier $e^{j2\pi\beta\tau_i t}$. Backscattering sensor node signals thus appear in the de-chirp outcome as a bandpass process centered around f_i as shown in Fig. 2.8. Thus, the time delay τ_i leads to a range-dependent subcarrier for the backscattered signal.

3.1.1 Enhanced Range Accuracy through Slow Rate Modulation

To maximize range estimation accuracy, a low-rate (compared to the waveform repetition frequency) preamble signal (e.g., 101010) is pre-pended to the sensor data.

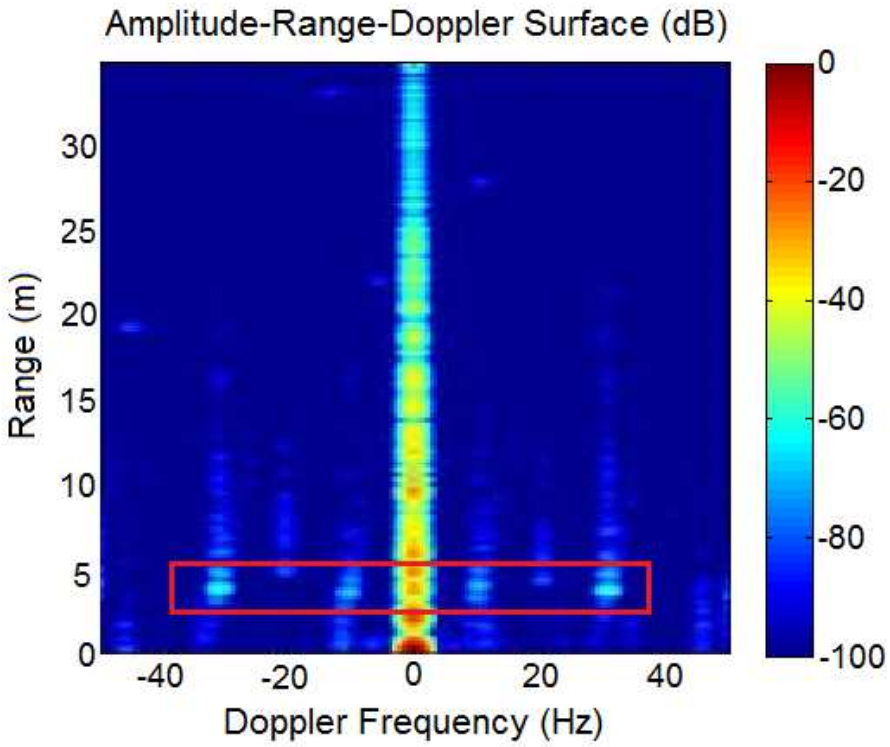


FIGURE 3.1: Measured amplitude-range-Doppler surface plot (dB) recovered from a node at 4 m sending the preamble (1010...) at $1/T_b = 10$ Hz and a chirp rate of $1/T_p = 1$ kHz

This preamble concentrates the signal energy from the sensor node within a small group of range bins to enhance the separation of the node return from ground clutter. An example of a range-Doppler surface for a backscattered continuous-preamble signal is shown in Fig. 3.1. In this figure, the sidebands of the node's response are seen in the highlighted area. The modulation due to the preamble pushes the node response away from the zero Doppler area dominated by stationary or near-stationary clutter.

3.2 FMCW Localization Performance Analysis Through the Averaged Cross-Ambiguity Function

The use of Frequency-Modulated Continuous-Wave (FMCW) allows to achieve simultaneous ranging and communication with backscatter transponder. The ability to estimate the range of such transponder depends on the radar waveform parameters. However, unlike in radar, the modulation alters the returned basckscatter. Range estimation then becomes non trivial, and its performance depends on the signaling parameters of the transponder. The radar ambiguity function (see Skolnik (2002)) has been used extensively to evaluate distortions in range and Doppler estimation of radar receiver. For radar, the lower bound on ranging estimation can be derived as a function of the ambiguity function of the radar system (see Trees (1992)). More precisely, it calculates the second partial derivative (the curvature) of the ambiguity manifold surface.

The ambiguity function in its basic form is

$$\chi(\tau, v) = \int_{-\infty}^{\infty} u(t)u^*(t-\tau)\exp\{-j2\pi vt\}dt \tag{3.5}$$

where τ is the time delay, v is the Doppler shift, $u(t)$ is the radar transmitted signal and * is the complex conjugate operation, and see Fig. 3.2.

In our case the 'target' is modulating, so traditional format of the ambiguity function does not encompass these structured fluctuations. If we assume that per single chirp, the sensor modulates M symbols, there are 2^M unique symbols sequences (for QPSK, 4^M). The Average Complex Ambiguity Function (ACAF) (see Stinco et al. (2012)) averages over all possible symbol sequences reflections. In addition, the sent and received signal are not symmetric, hence the use of the cross ambiguity function (see Cohen (1972)).

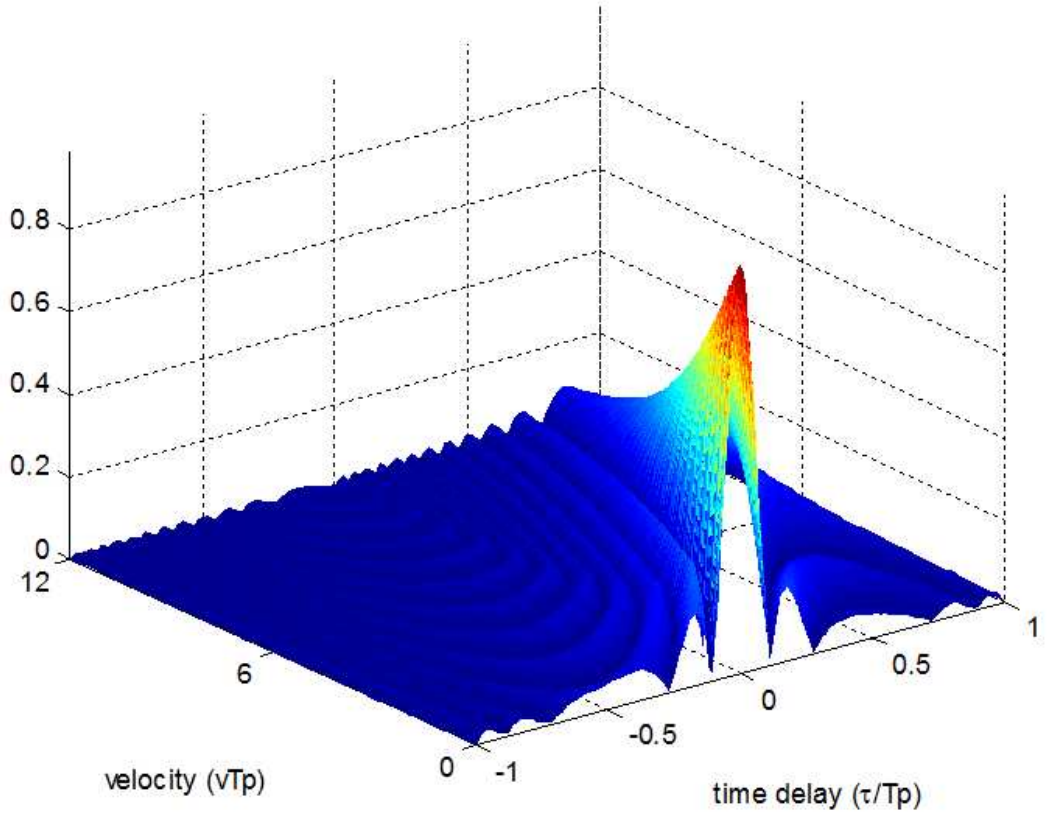


FIGURE 3.2: An ambiguity function of LFM pulse

The Average Complex Ambiguity Function (ACAF) takes the form of

$$\begin{aligned} \chi(\tau, v) &= E\{\chi_c(\tau, v)\} \\ \chi_c(\tau, v) &= \int_{-\infty}^{\infty} u(t) r_c^*(t, \tau) \exp\{-j2\pi v t\} dt \end{aligned} \tag{3.6}$$

where c is the sequence of symbols signaled by the tag and r_c is the received signal at the receiver containing the return radar signal and the tag modulation.

For the case of radar FMCW signal and modulating tag the Average Complex Ambiguity Function (ACAF) is derived. The unit energy complex envelope of the transmitted signal (a single FM pulse)

$$u(t) = \frac{1}{\sqrt{(T_p)}} \exp(j\pi \frac{B}{T_p} t^2) \text{rect}\Big[\frac{t}{T_p}\Big] \tag{3.7}$$

where B is the radar bandwidth, T_p is the radar pulse duration, T_b is the tag symbol duration, τ is the target delay, $M = T_p/T_b$ amd c_m is modulation of symbol m. The modulation signal of the RF tag is

$$m(t) = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} c_m p(t - mTb) \tag{3.8}$$

where for BPSK $c_m \in \{e^{j0}, e^{j\pi}\}$

The backscatterd received signal is (relative to receiver hypothesized time delay τ_H and veloctiy v_H)

$$s(t, \tau, v) = u(t - \tau) \exp(j2\pi vt) \cdot m(t) \tag{3.9}$$

The modified ambiguity function (for a given symbols sequence c)

$$\begin{aligned} \chi_c(\tau, v) &= \int_{-\infty}^{\infty} u(t) s^*(t, \tau) dt \\ &= \int_{-\infty}^{\infty} u(t) u^*(t - \tau) \exp(-j2\pi vt) m^*(t) dt \end{aligned} \tag{3.10}$$

Evaluating the absolute square value

$$|\chi_c(\tau, v)|^2 = \chi_c(\tau, v) \cdot \chi_c^*(\tau, v) \tag{3.11}$$

$$= \frac{1}{M^3} sinc^2(T_b\gamma) \cdot \sum_{m=0}^{M-1} \sum_{m=0}^{M-1} c_m^* c_n \exp[j2\pi T_b \gamma(m - n)] \tag{3.12}$$

where $\gamma \triangleq (\frac{B}{T_p}\tau - v)$

which can be viewed as the ambiguity function of radar FM pulse multiplied by the power spectral density (PSD) structure of RF tag signal $m(t)$ skewed by a factor of $(\frac{B}{T_p}\tau - v)$. A visual intuition can be seen in Fig. 3.3.

The following evaluations of the averaged complex ambiguity function, are drawn according to different parameters depending on the RF tag baseband signal modulation and the radar signal.

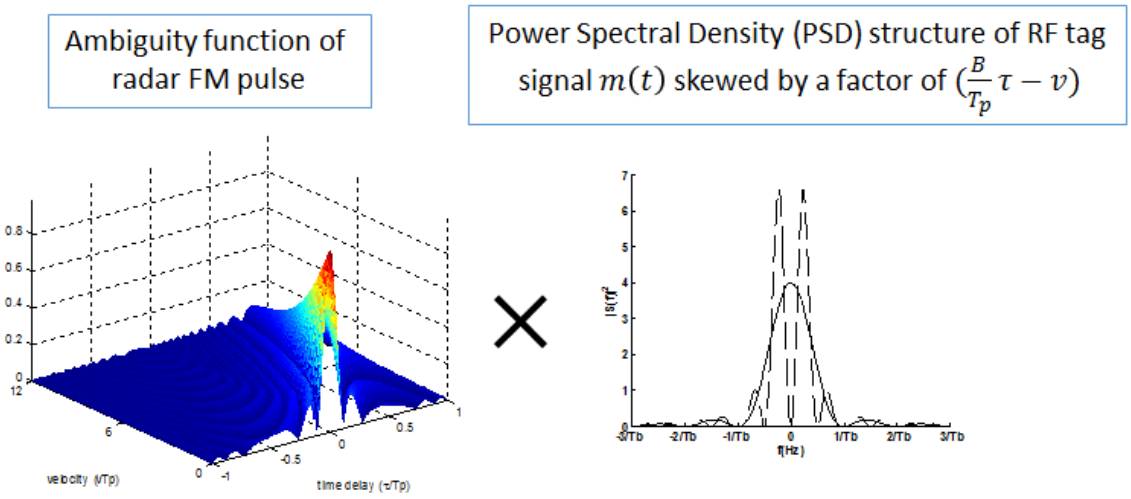


FIGURE 3.3: Cross ambiguity function of backscatter communication

ACAF of different symbol sequences (assuming $M = 8$ symbols per radar pulse) in Fig. 3.4

ACAF of different radar FM frequnecty sweep rate in Fig. 3.5

ACAF of different symbols rate in Fig. 3.6

ACAF of different symbol modulation scheme in Fig. 3.7

As can be validated from experimental measurements (see Fig. 3.8), a modulating tag at around 15 m using BPSK can demonstrate a central blub around its exact location and distinctive side lobes in range, unlike other static reflectors in the field of view of the radar.

3.2.1 Phase Modulated Baseband Averaged Power Spectral Density (PSD)

To evaluate better the term appearing in the ACAF, the power spectral density of the tag symbols is studied. It is assume that a phase modulation is used and that the symbols are uncorrelated (an assumption which is not true when using coding

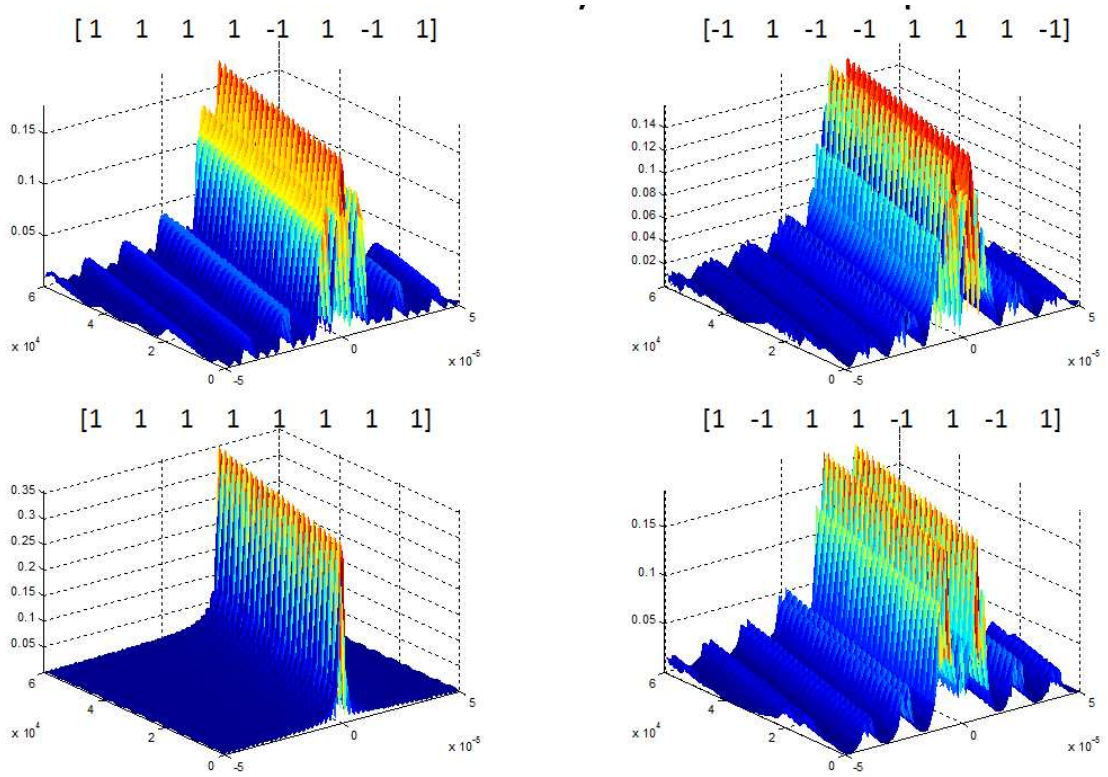


FIGURE 3.4: ACAF of different symbol sequences (assuming $M = 8$ symbols per radar pulse)

on the tag symbols). Signal model for M-ary digital modulation

$$s_c(t) = \sum_{m=0}^{M-1} Ac_m p(\frac{t}{T_b} - \frac{T_b(2m+1)}{2}) \tag{3.13}$$

where A is the signal amplitude, rectangular pulses are used $p(t) = \text{rect}\left[\frac{t}{T_b}\right]$ and the phase modulation (e.g. QPSK) is $c_m \in \{\exp(j\frac{\pi}{4}), \exp(j\frac{3\pi}{4}), \exp(j\frac{5\pi}{4}), \exp(j\frac{7\pi}{4})\}$

The power spectral density (PSD)

$$\psi_c(f) = A^2 T_b^2 sinc^2(\pi f T_b) \left| \sum_{m=0}^{M-1} c_m \exp[-j2\pi f \frac{T_b(2m+1}{2}] \right|^2 \tag{3.14}$$

for a given symbols sequence c

The averaged PSD, following the analysis in Stern and Mahmoud (2003)

$$\overline{\psi}(f) = E_c\{\psi_c(f)\} \tag{3.15}$$

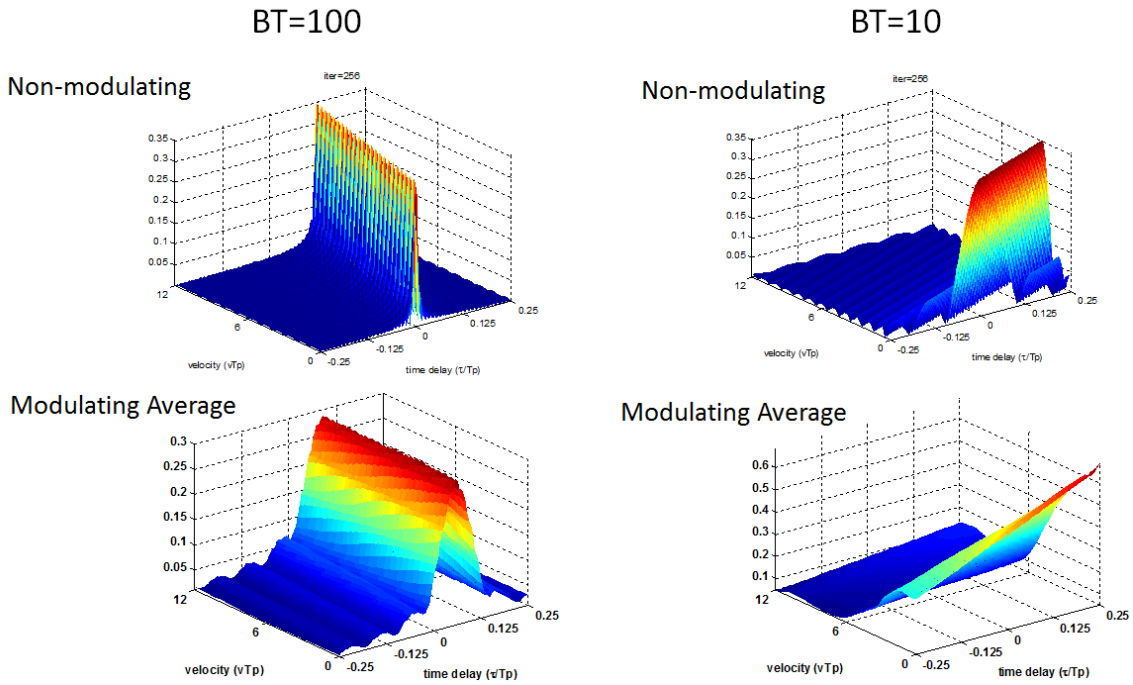


FIGURE 3.5: ACAF of different radar FM frequnecty sweep rate

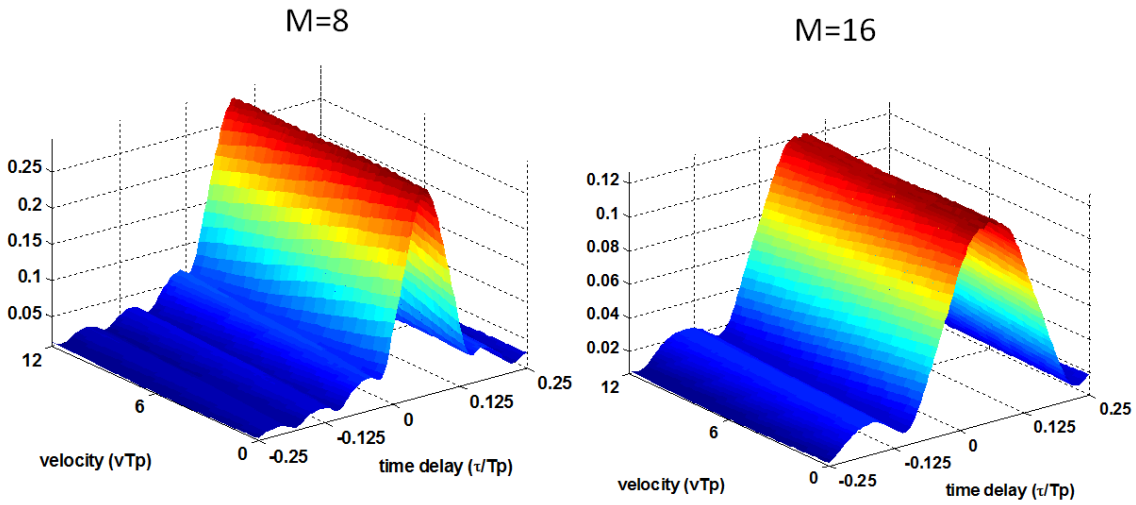


FIGURE 3.6: ACAF of different symbols rate

3.3 Fisher Information and the Cramér-Rao Lower Bound (CRB)

Using statistics, a problem can be modeled using a statistical model depending on some parameters.

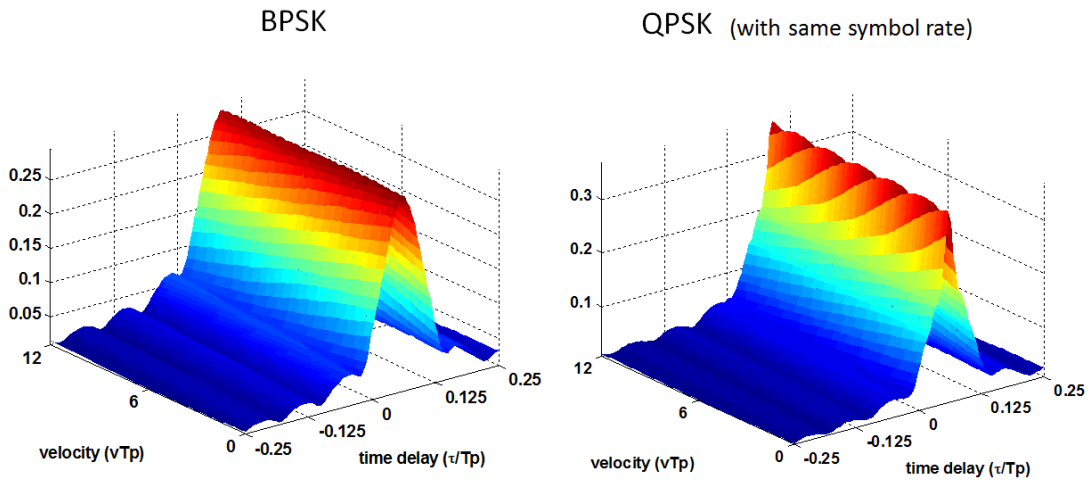


FIGURE 3.7: ACAF of different symbol modulation scheme

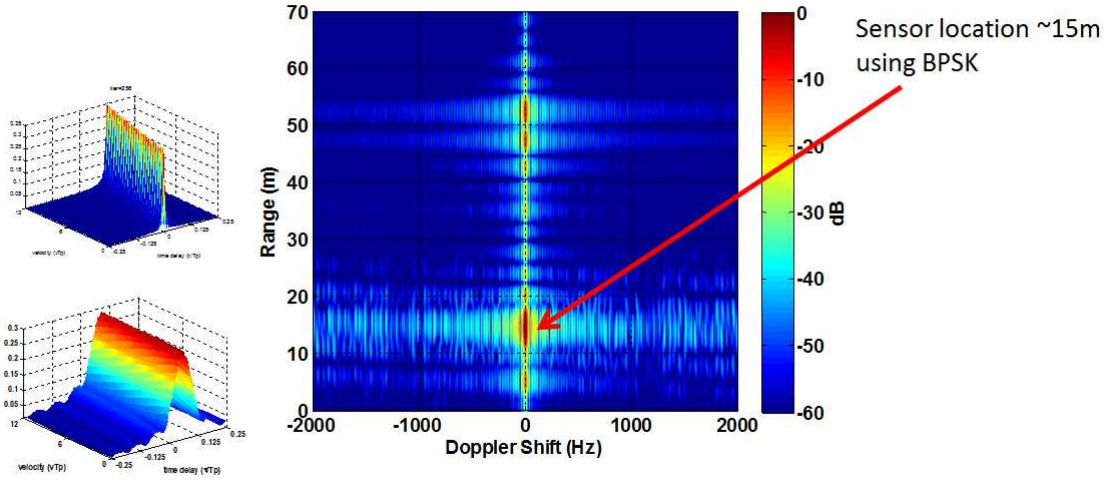


FIGURE 3.8: Validation against experimetnal results with parameters described in chapter 3

The likelihood function describes the statistical model of the problem with dependence on its parameters. Formally, a set of parameter values θ given outcomes x is equal to the probability of those observed outcomes given those parameter value

$$\mathcal{L}(\theta|x) = P(x|\theta) \tag{3.16}$$

In parametric inference we define a parametric model

$$\mathcal{P} = \{p(x|\theta) : \theta \in F\} \tag{3.17}$$

where $F \subset \mathbb{C}^k$ is the parameter space and $\theta = [\theta_1, ..., \theta_k]^T$ is the parameters vector. The goal of inference is defined as the estimation of θ from x. More formally

$$\hat{\theta} : \mathbb{C}^{n_x} \to \mathbb{R}^k \qquad x \mapsto \hat{\theta}(x) \tag{3.18}$$

Fisher information is a statistical tool that quantifies the amount of information carried in an observable random variable x about an unknown parameter θ, upon which the probability of x depends. Mathematically it is the variance of the expected value of the observed information. Fisher information is used for the asymptotic theory of maximum-likelihood estimation and can provide, using the Cramér-Rao lower bound, a metric on the performance of an unbiased estimator. The Fisher information matrix elements are defined as

$$[I(\theta)]_{ij} = -E\left[\frac{\partial^2 \log p(x|\theta)}{\partial\theta_i \partial\theta_j}\right] \tag{3.19}$$

The next step is measuring the performance of an unbiased estimator based on the Fisher information. When the regularity condition is satisfied

$$E\left[\frac{\partial \ln p(x|\theta)}{\partial\theta}\right] = 0 \qquad \forall\theta \tag{3.20}$$

Then the covariance matrix of unbiased estimator $\hat{\theta}$ satisfies

$$C_{\hat{\theta}} - I^{-1}(\theta) \succeq 0 \tag{3.21}$$

which means it is a positive semi-definite matrix. And the individual variance of the unbiased estimator $\hat{\theta}_i$ satisfies

$$\mathrm{var}(\hat{\theta}_i) \geqslant [I^{-1}(\theta)]_{ii} = -E\left[\frac{\partial^2 \log p(x|\theta)}{\partial\theta_i \partial\theta_j}\right] \tag{3.22}$$

where the derivative is evaluated at the true value of θ and the expectation is taken with respect to $p(x|\theta)$.

The bound term found is called the Cramér-Rao lower bound (CRB) which is a lower bound on the estimation error variance of any unbiased estimator. An unbiased estimator that can attain the bound $\forall\theta_{ii}$ (also called 'efficient estimator') may exist iff

$$\frac{\partial \log p(x|\theta)}{\partial \theta} = I(\theta) \cdot [\hat{\theta}(x) - \theta] \qquad \forall x \tag{3.23}$$

3.3.1 Fisher Information on Ranging at the De-Chirped Processing Output

We use Fisher information to quantify the amount of information carried in the modulated backscatter return of an RF tag about its range. Analyzing the Fisher information for the received signal model provides a complicated term. An alternative that allows a simpler analysis uses the model of receiver after the de-chirping processing.

It is therfore required to show that the de-chirping process preserves 'sufficient statistics' such that "no other statistic that can be calculated from the same sample provides any additional information as to the value of the parameter". By using Neyman-Fisher factorization of the likelihood function we can show it does preserve 'sufficient statistics' for the problem.

$$p(r|\tau) = g(T(r), \tau) \cdot h(r) \tag{3.24}$$

where r is the received signal, τ is the the tag time delay, $T(r)$ is the de-chirping process output and $h(r)$ is a residue which does not depend on τ

It is therefore possible to continue analysis of the Fisher information of the de-chirped process output, and ensure it is equivalent to the Fisher information of the directly received signal. In sum, we have translated the problem of estimating range information of modulating transponder from received backscatter into the problem of

estimating range information of modulating transponder from de-chirped backscatter.

It is important to emphasize here that there is some inherent difference between modeling the de-chirped output instead of the received signal. When the FMCW is correlated, the edges of the pulse are usually filtered out because of practical system implementation on the intermediate frequency (IF) of operation (and see section 2.2.3). The carrier frequency model does not have that effect, which for short ranges of delay is usually negligible. When FMCW is designed in an up and down fashion as described in 2.2.3, energy from the entire radar pulse can be considered and the models should be equivalent.

3.3.2 Signal Model of the De-Chirped Processing Output

A point target return is processed as a single complex tone carrier

$$s(t) = A \exp\{j\Big[2\pi f_d(t - t_0) + \theta\Big]\}\text{rect}\Big[\frac{t-\tau}{T_p}\Big] \tag{3.25}$$

where

A is the dechirped signal amplitude

$f_d \triangleq (\frac{B}{T_p}\tau_d)$ is the range induced carrier frequency

τ_d is the RF tag time delay

B is the radar bandwidth

T_p is the radar pulse duration

t_0 is a reference time of observation

θ is the carrier phase offset

rect$[\cdot]$ is the rectangular function

A modulating transponder is processed as baseband modulation centered around

a single carrier corresponding to the transponder range $f_c = \frac{B}{T_p}\tau$

$$s(t) = A\exp\{j\Big[2\pi\frac{B}{T_p}(t-t_0)+\theta\Big]\}\cdot m(t) \tag{3.26}$$

where

$m(t) = \sum_i c_i g(t - iT - \phi)$ is the RF tag modulation signal

c_i is the i$^{\text{th}}$ M-PSK symbol from a finite alphabet $\mathcal{A}$

$\mathcal{A} \triangleq \{0, 2\pi/M, ..., 2\pi(M-1)/M\}$ is the symbol alphabet

$g(t)$ is real valued signaling pulse

T is the symbol spacing

ϕ is the radar-tag jitter

T_0 is the observation window

and observe the signal in Fig. 3.9

For now assume added Additive White Gaussian Noise (AWGN) $w(t)$ with two-sided power spectral density $2N_0$ and no clutter/multipath.

$$r(t) = s(t) + w(t) \tag{3.27}$$

3.3.3 Fisher Information on Carrier Frequency Estimation of Linear Modulation

As described in (3.4), the output of the de-chirp process yields a corresponding complex tone whose frequency is a linear function of the time delay.

$$f_c = \frac{B}{T_p}\tau \tag{3.28}$$

It is therefore possible to state the problem of time delay as a problem of carrier frequency estimation. By using transformation of estimation parameters (see Kay (1993)), we can use the Fisher information developed for time-delay and extend it

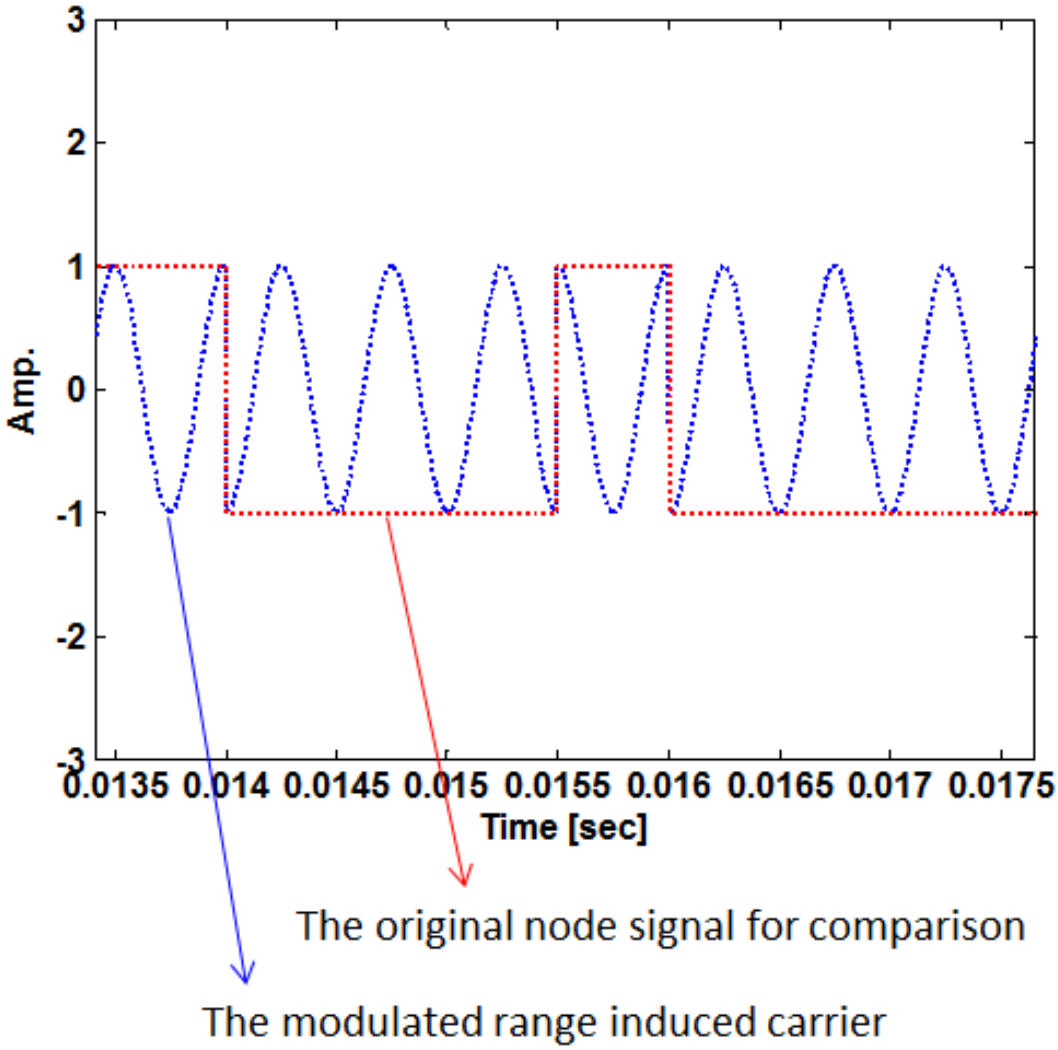


FIGURE 3.9: Modulated range induced carrier

to the problem of carrier frequency estimation

$$\text{var}(\hat{\tau}_d) = \frac{T_p^2}{B^2}\text{var}(\hat{f}_c) \tag{3.29}$$

In the same fashion the extension from time-delay to range is straightforward and is much more natural in radar literature

$$\Delta\text{range} = \frac{c}{2}\tau \tag{3.30}$$

where c is the speed of light. From here also follow the bound on error estimation

performance of unbiased estimator

$$\text{var}(\hat{\text{range}}) = \frac{c^2}{4}\text{var}(\hat{\tau}_d) = \frac{c^2 T_p^2}{4B^2}\text{var}(\hat{f}_c) \tag{3.31}$$

It is therefore possible to continue analysis of the Fisher information of the carrier frequency of passband modulation, and ensure it is equivalent to the Fisher information of the de-chirped process output. In sum, we have translated the problem of estimating range information of modulating transponder from received backscatter into the problem of estimating carrier frequency of passband modulation.

3.3.4 Development of the Fisher Information and Cramér-Rao Lower Bound (CRB) for Localization of FMCW with Modulated Backscatter

Assuming an observation window T_0 equals to the duration of a single radar pulse T_p, the likelihood function for a signal in white Gaussian noise Kay (1993)

$$\Lambda(\lambda, u_\lambda) = \exp\left[-\frac{1}{2N_0}\int_{T_0} |r(t) - s(t)|^2 dt \right] \tag{3.32}$$

where λ is the parameter to be estimated and u_λ are the unknown nuisance parameters (parameters we do not wish to estimate, yet are unknown).

The Fisher information for the scalar parameter λ is

$$I(\lambda) = -E_w\left\{ \frac{\partial^2[\log \Lambda(\lambda, u)]}{\partial \lambda^2} \right\} = \left[\frac{1}{N_0}\int_{T_0} \left| \frac{\partial s(t)}{\partial \lambda} \right|^2 dt \right] \tag{3.33}$$

where the expectation is with respect to the noise

The Fisher information is derived as follows

$$\frac{\partial}{\partial\lambda}(\ln\Lambda(\lambda,u)) = -\frac{1}{2N_0}\frac{\partial}{\partial\lambda}\left[\int_{T_0}|r(t)-s(t)|^2dt\right]dt$$

$$= -\frac{1}{2N_0}\int_{T_0}2Re\left[\frac{-\partial s(t)}{\partial\lambda}(r(t)-s(t))^*\right]dt$$

where * denotes the complex conjugate operation (3.34)

$$\frac{\partial^2}{\partial\lambda^2}(\ln\Lambda(\lambda,u)) =$$

$$\frac{1}{2N_0}\int_{T_0}2Re\left[\frac{\partial^2 s(t)}{\partial\lambda^2}(r(t)-s(t))^*\right] - 2\left|\frac{\partial s(t)}{\partial\lambda}\right|^2 dt$$

Taking the expectation with respect to the noise

$$I(\lambda) = -E_w\left\{\frac{\partial^2}{\partial\lambda^2}(\ln\Lambda(\lambda,u))\right\} = \frac{1}{N_0}\int_{T_0}\left|\frac{\partial s(t)}{\partial\lambda}\right|^2 dt \tag{3.35}$$

The Cramér-Rao lower bound (CRB) for the parameter λ is derived, providing a lower bound on the error estimation of for any unbiased estimator:

$$\mathrm{CRB}(\lambda) \geqslant I^{-1}(\lambda) = \left[\frac{1}{N_0}\int_{T_0}\left|\frac{\partial s(t)}{\partial\lambda}\right|^2 dt\right]^{-1} \tag{3.36}$$

Developing the CRB for time-delay estimation $\hat{\tau}_d$

$$\mathrm{CRB}(\hat{\tau}_d) \geqslant \left[\frac{4A^2\pi^2}{N_0}\frac{B^2}{T_p^2}\int_{T_0}\left|(t-t_0)\sum_i c_i g(t-iT-\phi)\right|^2 dt\right]^{-1} \tag{3.37}$$

3.4 Cramér-Rao Lower Bound (CRB) and Maximum-Likelihood Estimator for Localization of FMCW with Modulated Backscatter

This section will provide the specific derivation of the CRB and MLE or their approximations for different important cases of tag modulation.

3.4.1 CRB for the Case of Modulation Rate Is Zero

Tag modulation is constant, behaving as a point reflector. Using the same model of modulated received signal, we set c_i to be of constant value, without loss of generality we set it to be of unit value. We also assume the symbol pulse $g(t)$ to be of 100% duty cycle, which is a reasonable assumption for continuous switching base RF tags. The derived CRB (choosing t_0 in to middle of T_0 to maximize the term)

$$\begin{aligned}
\mathrm{CRB}(\hat{\tau}_d) &\geqslant \left[\frac{4A^2\pi^2}{N_0} \frac{B^2}{T_p^2} \int_{T_0} \left| (t-t_0) \sum_i c_i g(t - iT - \phi) \right|^2 dt \right]^{-1} \\
&= \left[\frac{4A^2\pi^2}{N_0} \frac{B^2}{T_p^2} \int_{T_0} \left| (t-t_0) \right|^2 dt \right]^{-1} = \left[\frac{4A^2\pi^2}{N_0} \frac{B^2}{T_p^2} \frac{T_0^3}{12} \right]^{-1} \\
&= \left[\frac{A^2\pi^2 B^2 T_0}{3N_0} \right]^{-1}
\end{aligned} \tag{3.38}$$

remembering the observation window T_0 is equal to the duartion of a single radar pulse T_p.

The result is linear with the LFM bandwidth squared B^2. It is linear with the signal to noise ratio defined as the energy of the received radar pulse $E_{LFM} = A^2 T_p$ divided by the noise spectral density N_0. It is also linear with the observation window.

The result can also be observed from the perspective of carrier frequency estimation

$$\mathrm{CRB}(\hat{f}_c) \geqslant \left[\frac{A^2\pi^2 T_0^3}{3N_0} \right]^{-1} \tag{3.39}$$

such that the bound depends on the observation window cubed T_0^3

3.4.2 Evaluation of the Fisher Information for the Case of Modulation Rate Is Zero

We now observe the result for the range estimation performance in light of other bounds in the literature.

The first is the bound developed for normalized frequency estimation of a complex sinusoid in noise (see Rife and Boorstyn (1974)). The CRB developed for that case

$$\mathrm{CRB}(\hat{f}_c) \geqslant \left[\frac{b_0^2 T_s^2 N(N^2-1)}{12\sigma^2} \right]^{-1} \tag{3.40}$$

where b_0 is the received signal amplitude, T_s is the sampling rate, N is the number of samples and remembering that the observation window is $T_0 = N \cdot T_s$

The bound has a similar dependencies as with the bound derived above, especially the dependency on the observation window cubed, .

A second bound to compare with is the bound developed for the radar time delay estimation (see Trees (1992) and Richards (2005))

$$\mathrm{CRB}(\hat{\tau}_d) \geqslant \left[\frac{8\pi^2 E_s \beta_{rms}^2}{\sigma_w^2} \right]^{-1} \tag{3.41}$$

where E_s is the radar pulse energy that for LFM equals $E_s = A^2 T_0$, $\beta_r ms$ which is defined as $\beta_r ms = \sqrt{\frac{\int_{-\infty}^{\infty} f^2 |S(f)|^2 df}{\int_{-\infty}^{\infty} |S(f)|^2 df}}$ that for LFM equals $\beta_r ms^2 = \frac{B^2}{12}$ and σ_w^2 is the noise variance.

Again, the bound share the same dependencies as the bound developed above.

A third comparison is done against the Maximum-Likelihood Estimator (MLE). An MLE for the problem of carrier frequency estimation of a sinusoid was pursued in Rife and Boorstyn (1974). It has been shown that even for the a single-tone frequency estimation with no modulation, the MLE cannot be found analytically. An approximation uses a two-step algorithm: coarse estimation based on maximization of the periodogram, and finer search using numerical analysis to find local maximum point.

For the case of a modulating target with use of FMCW the MLE is derived:

$$\hat{f}_{c,MLE} = \underset{f_c}{\operatorname{argmax}}\ \Lambda(f_c) \tag{3.42}$$

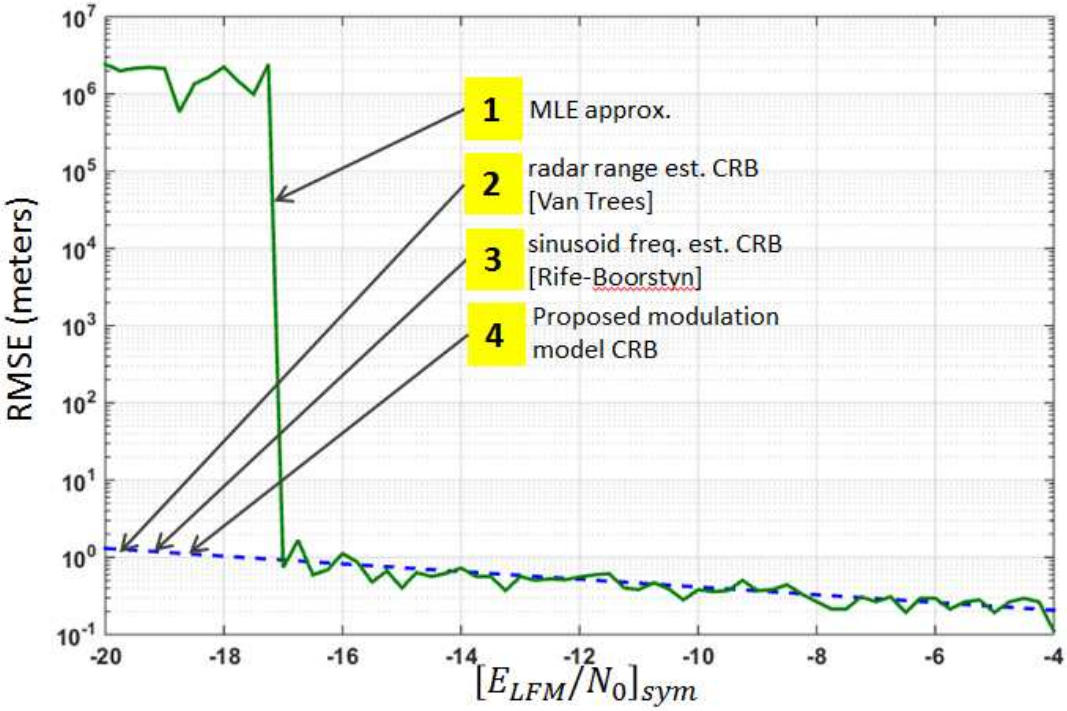


FIGURE 3.10: Case of modualtion rate is zero

where

$$\Lambda(f_c) = \int_{T_0} (t - t_0)\Re\{A\exp[2\pi f_d(t - t0) + \theta] \cdot m(t) \cdot r^*(t)\}dt \tag{3.43}$$

and

$$m(t) = \sum_i c_i g(t - iT - \phi) \tag{3.44}$$

Comparison of the different bounds and simulation results for an approximation of the MLE using the maximization of the periodogram can be seen in Fig. 3.10. As can be seen, the simulation results of the approximation to the MLE estimator attains the bound for values of E_{LFM}/N_0 greater than about -17 dB (normalized for a symbol duration of $T = T_p/1000$).

3.4.3 CRB for the Case of Message Known to Reader (Pilot/Preamble)

Tag modulation follows a sequence of symbols, known to the receiver. This sequence is sometimes called a pilot sequence or a preamble being sent just before actual data is sent. In order to incorporate the knowledge of the receiver, we can assume the receiver first mix the receiver processed de-chirp output with the conjugate known baseband signal.

$$\begin{aligned} s'(t) =& A\exp\{j\Big[2\pi\frac{B}{T_p}(t-t_0)+\theta\Big]\}\cdot m(t)\cdot m*(t) \\ =& A\exp\{j\Big[2\pi\frac{B}{T_p}(t-t_0)+\theta\Big]\} \end{aligned} \tag{3.45}$$

3.4.4 Evaluation of the Fisher Information for the Case of Message Known to Reader

The result is similar to the case of signal model used in modulation rate equals zero. Therefore the resulting bounds are the same as well.

$$\begin{aligned} \mathrm{CRB}(\hat{\tau}_d) \geqslant& \left[\frac{4A^2\pi^2}{N_0}\frac{B^2}{T_p^2}\int_{T_0}\left|(t-t_0)\sum_i c_i g(t-iT-\phi)\right|^2 dt\right]^{-1} \\ =& \left[\frac{4A^2\pi^2}{N_0}\frac{B^2}{T_p^2}\int_{T_0}\left|(t-t_0)\right|^2 dt\right]^{-1} = \left[\frac{4A^2\pi^2}{N_0}\frac{B^2}{T_p^2}\frac{T_0^3}{12}\right]^{-1} \\ =& \left[\frac{A^2\pi^2B^2T_0}{3N_0}\right]^{-1} \end{aligned} \tag{3.46}$$

remembering the observation window T_0 is equal to the duration of a single radar pulse T_p.

The result is linear with the LFM bandwidth squared B^2. It is linear with the signal to noise ratio defined as the energy of the received radar pulse $E_{LFM} = A^2T_p$ divided by the noise spectral density N_0. It is also linear with the observation window.

The result can also be observed from the perspective of carrier frequency estimation

$$\mathrm{CRB}(\hat{f}_c) \geqslant \left[\frac{A^2 \pi^2 T_0^3}{3N_0} \right]^{-1} \tag{3.47}$$

such that the bound depends on the observation window cubed T_0^3

The bound is identical to the case of non-modulating transponder. Knowledge of the modulating sequence removed uncertainty from the received signal, allowing a theoretical performance of an non-modulating transponder.

The MLE for this case cannot be found analytically, similarly to the case of a carrier frequency estimation of sinusoid without modulation. An approximation to the MLE following the lines of Rife and Boorstyn (1974) uses the periodogram once again. The concept of the estimator can be found in Fig. 3.11. The received signal is cross-correlated in the frequency domain with a spectrum 'mask' of the known baseband modulation, based on knowledge of the symbols sequence c. This concept can be seen as implementation of the matched filter (MF) to the symbols sequence, that is validated at different time delay hypotheses, and chooses the hypothesis with the highest detection output.

Comparison of the bound and simulation results for an approximation of the MLE using the maximization of the periodogram based on the symbols sequence pulses can be seen in Fig. 3.12. As can be seen, the simulation results of the approximation to the MLE estimator attains the bound for values of E_{LFM}/N_0 greater than about -17 dB (normalized for a symbol duration of $T = T_p/1000$).

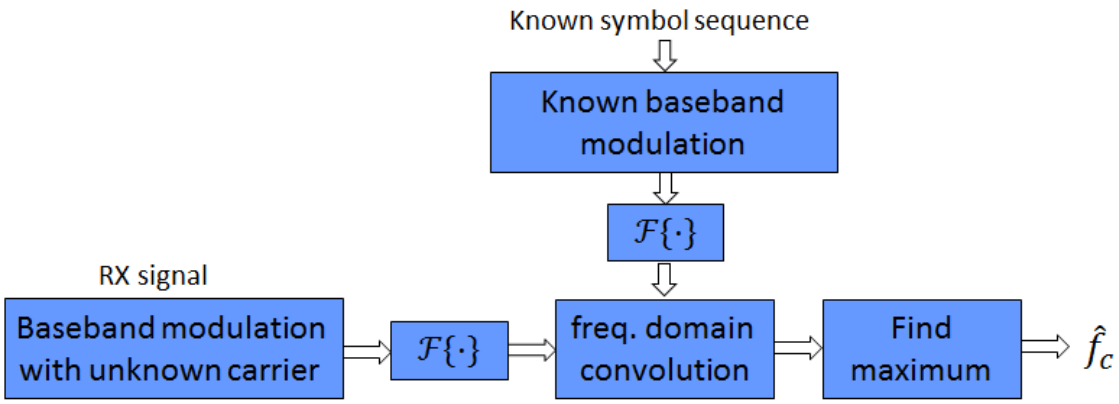


FIGURE 3.11: Estimator approximating the MLE

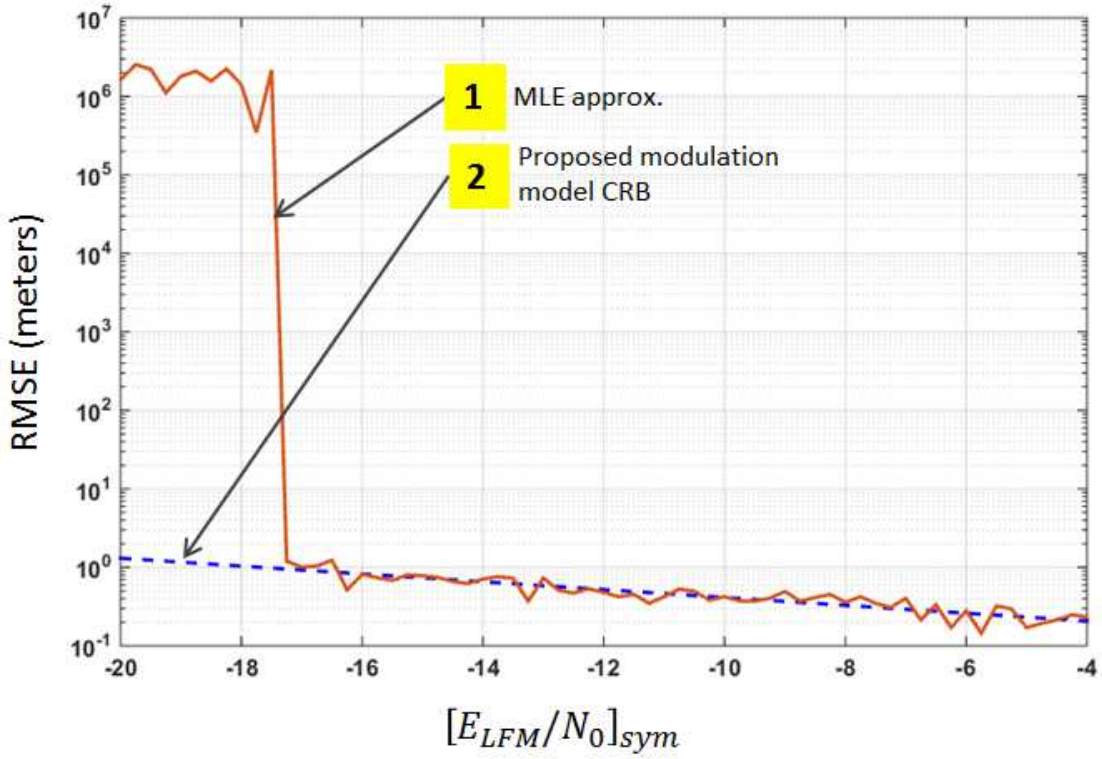


FIGURE 3.12: Case of constant message sent

3.4.5 CRB for the Case of Message Unknown to Reader

Tag modulation follows a sequence of symbols in M-PSK, unknown to the receiver and are uncorrelated.

$$E\{c_k c_i^*\} = \begin{cases} M_2 & i = k \\ 0 & \text{elsewhere} \end{cases} \tag{3.48}$$

where M_2 is the autocorrelation of the symbols, and for BPSK $M_2 = 1$. We also assume the symbol pulse $g(t)$ to be of 100% duty cycle, which is a reasonable assumption for continuous switching base RF tags.

The likelihood function for this case needs to account for different sequences of symbols, which makes the computation of CRB non-analytical. An alternative bound, the modified CRB (MCRB) (see D'Andrea et al. (1994)), employs a statistical model on the tag message and incorporate its structure in the likelihood function. The result provides a more representative bound of the problem, but looser than the true CRB.

$$MCRB(\lambda) \leqslant CRB(\lambda) \tag{3.49}$$

The MCRB takes in the general form of

$$MCRB(\hat{\tau}_d) = \left[E_{\bar{c}} \left\{ E_{w|\bar{c}} \left[\left(\frac{\partial \log p(r|\tau_d, \bar{c})}{\partial \tau_d} \right)^2 \right] \right\} \right]^{-1} \tag{3.50}$$

Developing the MCRB for time-delay estimation $\hat{\tau}_d$

$$MCRB(\hat{\tau}_d) = \left[E_{\bar{c}} \left\{ E_{w|\bar{c}} \left[\left(\frac{\partial \log p(r|\tau_d, \bar{c})}{\partial \tau_d} \right)^2 \right] \right\} \right]^{-1}$$

$$= \left[E_{\bar{c}} \left[\frac{1}{N_0} \int_{T_0} \left| \frac{\partial s(t, \bar{c})}{\partial \tau_d} \right|^2 dt \right] \right]^{-1}$$

$$= \left[E_{\bar{c}} \left[\frac{4A^2\pi^2}{N_0} \frac{B^2}{T_p^2} \int_{T_0} \left| (t - t_0) \sum_i c_i g(t - iT - \phi) \right|^2 dt \right] \right]^{-1} \tag{3.51}$$

$$= \left[\frac{4A^2\pi^2}{N_0} \frac{B^2}{T_p^2} \int_{T_0} (t - t_0)^2 \right.$$

$$\left. \cdot \sum_i \sum_k E_{\bar{c}}[c_i c_k] g(t - iT - \phi) g(t - kT - \phi) dt \right]^{-1}$$

and since the symbols are uncorrelated, and the symbol pulse $g(t)$ is of 100% duty cycle

$$MCRB(\hat{\tau}_d) = \left[\frac{4A^2\pi^2}{N_0} \frac{B^2}{T_p^2} \int_{T_0} (t - t_0)^2 \cdot \sum_i E_{\bar{c}}[c_i c_i^*] g(t - iT - \phi) dt \right]^{-1} \tag{3.52}$$

$$= \left[\frac{4A^2\pi^2 M_2}{N_0} \frac{B^2}{T_p^2} \frac{T_0^3}{12} \right]^{-1} \tag{3.53}$$

remembering that the observation window T_0 equals a single radar pulse duration T_p and that for M-PSK $M_2 = 1$ we conclude with

$$MCRB(\hat{\tau}_d) = \left[\frac{A^2\pi^2 B^2 T_0}{3N_0} \right]^{-1} \tag{3.54}$$

3.4.6 Evaluation of the Fisher Information for the Case of Message Unknown to Reader

The result for the looser bound (the MCRB) are similar to the case of no modulation rate equals zero. This is not surprising, as no modulation is the optimal case for range

estimation (no symbol distortions imposed by modulation). Since the MCRB is a looser bound than the CRB, by averaging the Fisher information over all symbol sequences, it indicates that the true CRB is higher (or equal). This makes sense, as we know that the tag modulation causes a performance degradation on the range estimation.

The result is linear with the LFM bandwidth squared B^2. It is linear with the signal to noise ratio defined as the energy of the received radar pulse $E_{LFM} = A^2 T_p$ divided by the noise spectral density N_0. It is also linear with the observation window.

The result can also be observed from the perspective of carrier frequency estimation

$$\mathrm{CRB}(\hat{f}_c) \geqslant \left[\frac{A^2 \pi^2 T_0^3}{3 N_0} \right]^{-1} \tag{3.55}$$

such that the bound depends on the observation window cubed T_0^3

The MLE for this case cannot be found analytically, similarly to the case of a carrier frequency estimation of sinusoid without modulation. An approximation to the MLE follows the lines of Rife and Boorstyn (1974) and Gardner method (see Karam et al. (1995)). The concept of the estimator can be found in Fig. 3.13. The received signal is cross-correlated in the frequency domain with a spectrum 'mask of the known modulation pulse, as there is no knowledge on the actual symbols sequence c. This concept can be seen as implementation of the matched filter (MF) to the symbol pulse, that is validated at different time delay hypotheses, and chooses the hypothesis with the highest detection output.

Other advanced estimators in literature exploring the problem of frequency estimation using complex feedback loop structure and use of derivative matched filter (FMF) along the MF to approximate the MLE. Unfortunately, their performance are "quite far from MCRB [and some] attain the limit under some restrictive conditions." (see D'Andrea et al. (1994)).

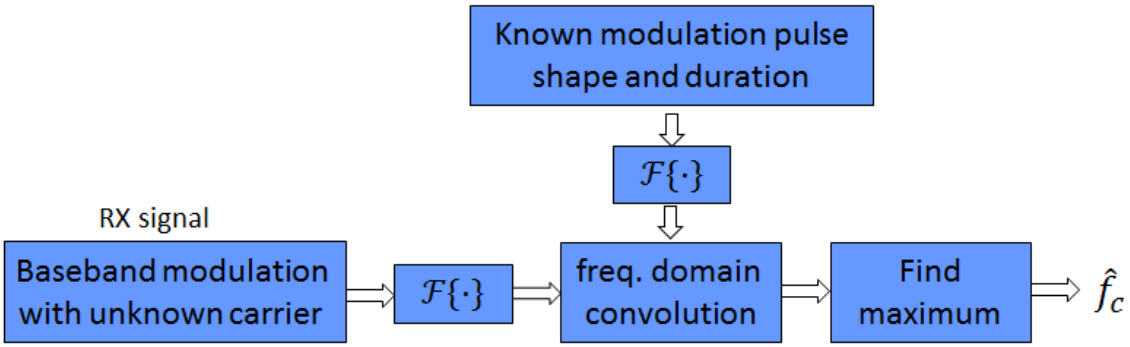


FIGURE 3.13: Estimator approximating the MLE

Comparison of the bound and simulation results for an approximation of the MLE using the maximization of the periodogram based on the pulse duration can be seen in Fig. 3.14. As can be seen, the simulation shows Root Mean Square Error (RMSE) results of the approximation to the MLE estimator for two different rates of symbols: 1000 symbols per single radar pulse and 250 symbols per single radar pulse. As can be seen the estimator performs better with lower rate of tag modulation. It should be noted that although the difference between the estimator results and the modified bound is quite high (35-45 dB), we must not forget that the MCRB looser bound on the true CRB, and that the estimator used is an approximation of the MLE, so the real gap between the true CRB and the exact MLE is probably smaller, which should encourage future work.

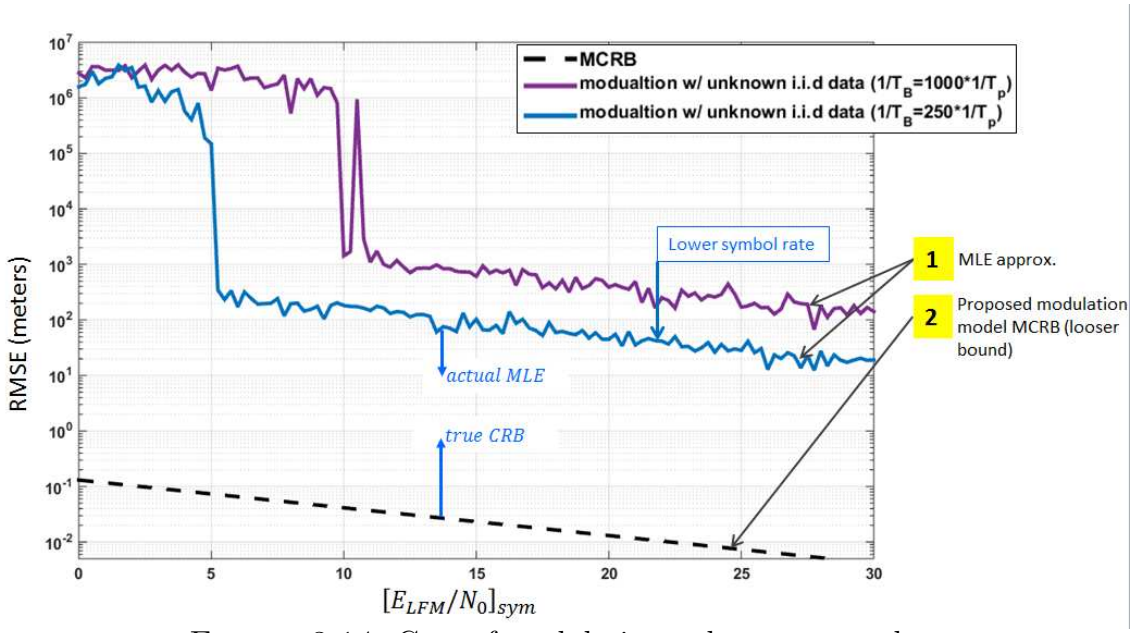


FIGURE 3.14: Case of modulation unknown to reader

4

Quasi-Cooperative Range and Channel Coding

This chapter introduces a recent development of the work of previous chapters by leveraging the use of coding. A slightly different signal and channel model is used which is more suitable to the coding problem domain and has relaxed some assumptions of previous model. The motivation however remains the same: analyzing and providing clutter mitigation and performing precise ranging in backscatter communication.

4.1 Introduction

A backscatter system operates in the dyadic backscatter channel, a pinhole channel composed of a forward and backscatter link (see Griffin and Durgin (2008)). The dyadic backscatter channel poses unique challenges that are inherently different than one-way conventional channels and provides a rich and unique set of theoretical research problems. The backscatter channel exhibits extreme self-interference (clutter) reflections masking the weak modulated backscatter return signal by several orders of magnitude (see Lasser and Mecklenbrauker (2015)). As a result, recovery of the RF tag data communication and accurate estimation of the range to the RF tag

become difficult.

In order to achieve acceptable receiver sensitivity while operating in the backscatter channel, a key element of clutter filtering (i.e. pulse subtraction and see section 2.5) needs to be addressed as a first step at the receiver front end, preferably before sampling to avoid receiver saturation and dynamic range limitations. This operation however, creates impairment which affects all signals passing through the channel.

Consequently, coding employed at the RF tag for data communication or ranging purposes must consider the effective channel that now includes the clutter filtering operation. We propose coding that takes into account the new effective channel and allows a capable receiver to reconstruct the original coding sequence.

Previous work have explored the use of coding in the backscatter channel. Error correcting codes were employed to increase the range of operation (see Alevizos et al. (2014)) and space-time coding that requires additional antennas at the reader and the RF tag has been proposed (see Boyer and Roy (2013)). A more channel specific work considered coding for the case of simultaneous tag energy harvesting and data communication (see Tandon et al. (2014)). Clutter mitigation for the backscatter channel was addressed in works proposing hardware additions to the RF tag that avoid lower frequencies dominated by clutter. Such were the addition of a local oscillator (see Carlowitz et al. (2013)), or the use of multiple antennas on the reader and the tag (see Boyer and Roy (2013)). Other methods (see Lee et al. (2007); Safarian et al. (2007)) have focused on active cancellation of two dominant returns (internal TX-RX reader leakage and antenna TX-RX direct blast).

The EPC Gen-2 protocol, which standardizes radio-frequency identification (RFID) systems, offers two coding methods: Miller code and FM0. Both codes operate at a maximum rate of 1/2 designed to mitigate static clutter, but are limited to reader signals based on a continuous wave (CW) (see EPC Global US (2005)). More recent work (see chapter 2) studied the use of specific pulse based linear frequency modu-

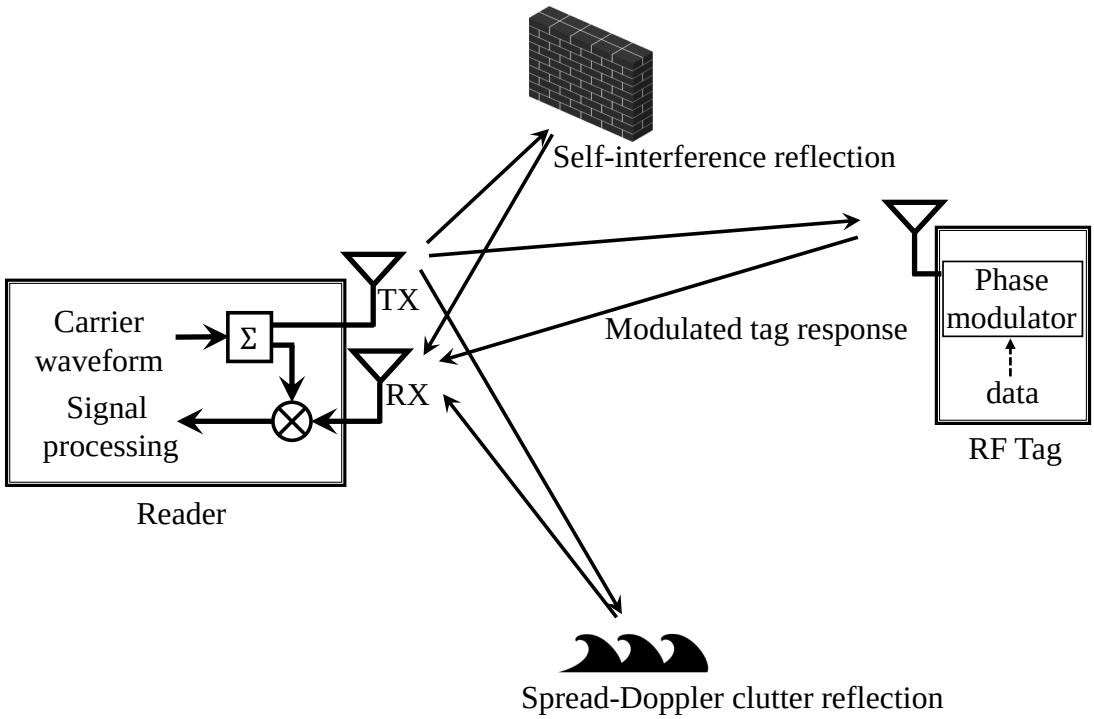


FIGURE 4.1: Backscatter communication between RF tag and a reader with common channel interferences

lated (LFM) waveforms from the reader and using differential coding at rate 1, but this work was targeted at static clutter mitigation only (see Cnaan-On et al. (2015)).

Ranging estimation of backscatter tags has been studied in previous works as well. Phase based synthetic aperture has been proposed for CW (see Miesen et al. (2013)). Other phase based method considered dual CW reader (see Zhou and Griffin (2012)). Ranging using direct sequence spread spectrum (DSSS) (see Arthaber et al. (2015)) and LFM based methods (see Carlowitz et al. (2013); Cnaan-On et al. (2015)) have been studied as well but with some degree of interference caused by the tag modulation.

4.2 Backscatter communication channel model and signal processing

4.2.1 Backscatter communication processing overview

Backscatter communication in its most simple design consists of a reader and an RF tag that signals data as shown in Fig. 4.1. The carrier signal consists of an interrogation transmitted waveform generated by the reader. Usually it is assumed the RF tag is not synchronized with the reader. As a result, the reader would not know when to expect a tag message. In order to maintain constant on-line communication, it is necessary for the reader to continuously generate a waveform to carry back the tag modulations. The illuminating waveform can be either a continuous wave (CW), which consists of a pure sinusoid with continuous phase (see Curty et al. (2007)), or as recently proposed and see chapter 2, a pulse train waveform. The framework developed in this paper is general and applies to either waveform type.

The signal transmitted by the reader is

$$s(t) = \sum_{n=-\infty}^{\infty} p(t - nT_p) \tag{4.1}$$

where $p(t)$ is a time-limited single pulse such that

$$p(t) = 0 \text{ , when } t \leqslant 0 \cup T_p \leqslant t \tag{4.2}$$

and T_p is the pulse duration. This general signal model also applies for CW, as long as the pulse $p(t)$ consists of an integer number of sinusoid wavelengths, such that the continuous phase is maintained from pulse to pulse.

The RF tag modulation is generated by a phase modulator connected to an antenna as shown in Fig. 4.1. It is assumed that the RF tag has its own energy supply that provides the energy required for the operation of the modulator . A portion of the incident interrogation signal is reflected, phase modulated and re-radiated back to the reader. This operation allows information to be sent from the

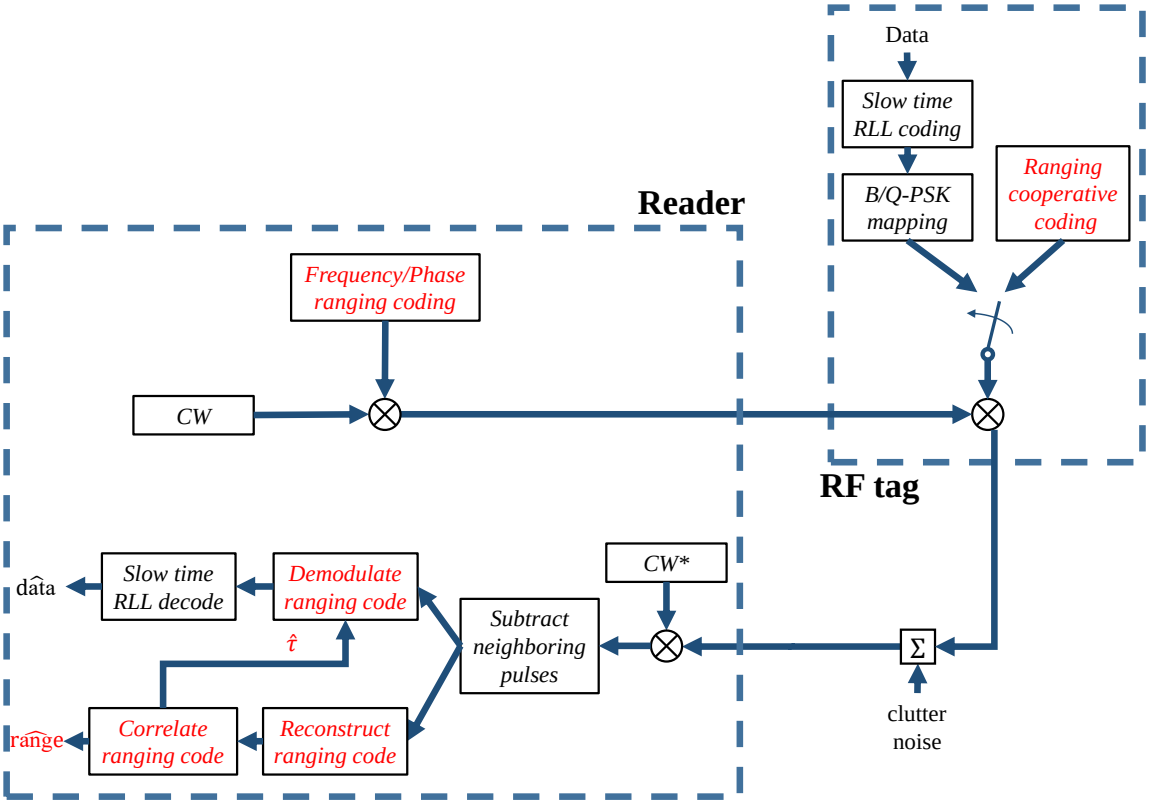


FIGURE 4.2: Processing chain of simultaneous communication and time-delay estimation.

tag to the reader (tag→reader). Information sent in the other direction (reader→tag) is not covered in the scope of this work. This work also assumes that the RF tag and the reader are either stationary or moving slowly such that the respective Doppler frequency shift is negligible within a single pulse period.

The message signal driving the RF tag's modulator is

$$m(t) = \sum_{k=-\infty}^{\infty} a_k \cdot q(t - kT_s) \tag{4.3}$$

where a_k is a constellation symbol from a finite symbol alphabet such as BPSK constellation, and $q(t)$ is a rectangular pulse of the symbol duration T_s representing a single symbol period.

The reflected backscatter signal from the RF tag received at a bi-static reader is

$$r(t) = \alpha(r_n) \cdot \sum_{n=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} p(t - nT_p - \tau) \cdot a_k \cdot q(t - kT_s - \phi) + n(t) \tag{4.4}$$

where $\alpha(r_n)$ is the attenuation due to the two-way backscatter path of length r_n, τ is the time delay associated with the two-way backscatter path of length r_n, ϕ is the phase delay between the reader clock and the tag's clock and $n(t)$ is an additive white Gaussian noise (AWGN).

Multiple tags can operate simultaneously, either by employing some time division algorithm (see Lee et al. (2005)) or leveraging the time-bandwidth-product of the wideband interrogating signal for time delay separation (see Cnaan-On et al. (2015)). This chapter will not address specifically multiple tags operation simultaneously, but the current methods for multiplexing (see section 2.6) do not restrict or limit any changes made to the data message or waveform code which are the domain of the proposed coding framework.

For data recovery purposes, the reader processes the received signal with the goal of extracting the binary message signal of the tag. The reader performs initially a correlation of the received signal with a conjugated copy of the interrogation signal. This allows removal of the reader carrier signal. However, when a pulse train is used as an interrogating waveform, intermediate steps also requires the reader to estimate the two-way propagation time delay τ and reconstruct the waveform code. These steps ensure that the correlation outcome is eventually identical to that of the continuous wave. Time-delay estimation and involved processing are analyzed separately in section 4.4.

After processing, the tag signal is the same as a conventional phase modulated

signal

$$u(t) = r(t) * s^*(t) = \alpha(r_n) \sum_{k=-\infty}^{\infty} a_k \cdot q(t - kT_s - \phi) + \tilde{n}(t) \tag{4.5}$$

where $\tilde{n}(t)$ is AWGN.

4.2.2 Clutter and fading in backscatter communication

In conventional one-way communication, we are usually concerned with interference that is the result of the signal of interest interfering with itself and causing multipath channel fading. In backscatter communication, the situation is drastically different, as the majority of interference is from reflections of the illuminating reader signal in the environment, manifesting as self-interference and spread-Doppler clutter. These interferences, inherently unique to backscatter communication have a very distinctive signal structure that is highly correlated with the reader rather than the signaling RF tag message signal. Another factor to consider is that the signal to interference ratio is orders of magnitude weaker (see Griffin and Durgin (2009a)) than what is usually found in a conventional one-way communication channel. Consequently, clutter mitigation needs to be addressed first, preferably in the analog domain prior to sampling and digitization to avoid receiver saturation, only then can the multipath be addressed using methods explored in the literature (see Fawky et al. (2014)).

4.2.3 Self-interference

Self-interference is a result of the reader's illuminating signal propagating, reflecting and scattering (sometimes multiple times) from static elements in the environment or caused by an internal leakage from the transmitter to the receiver circuitry. At the reader input, every reflection will exhibit a phase shift corresponding to the traveled

path delay

$$r(t) = \sum_{n=-\infty}^{\infty} \sum_{q=1}^{Q} \alpha(r_q) p(t - nT_p - \tau_q) \tag{4.6}$$

where Q is the number of static clutter returns, $\alpha(r_q)$ is the attenuation due to the two-way backscatter path of length r_q, and τ_q is the time delay associated with the two-way backscatter path of length r_q.

For CW, after the initial processing of cross-correlation with the conjugate interrogation signal at the reader, each of the reflections will contribute some DC magnitude offset corresponding to its phase, which is constant over time

$$u(t) = r(t) * s^*(t) = \sum_{q=1}^{Q} \alpha(r_q) \phi(\tau_q) \tag{4.7}$$

where ϕ is a DC magnitude offset corresponding to the phase difference caused by the time delay τ_q.

For pulse train, after the initial processing of cross-correlation with the conjugate interrogation signal at the reader, the output for the sum of the reflections will be a signal pattern $D_q(t)$ time limited between $0 \leqslant t \leqslant T_p$ that is repeating at the pulse duration T_p intervals (see Fig. 2.4).

$$u(t) = r(t) * s^*(t) = \sum_{q=1}^{Q} \alpha(r_q) D_q(t - \tau_q) \tag{4.8}$$

When considering any practical system, an assumption of a completely static environment can not hold. Backscatter channel measurements exhibit some degree of Doppler spread, as evident in the measurements in Cnaan-On et al. (2015) and therefore a different model of clutter is needed.

4.2.4 Spread-Doppler clutter

Spread-Doppler clutter is the result of the illuminating signal reflecting in a dynamic environment, which include sources of movement such as turbulence and other small-

scale flows (see Ramakrishnan and Krolik (2009)). With greater power and ranges of operation, the resulting channel is more exposed to spread Doppler effects from movements in the extended environment.

After the receiver processing, the spread-Doppler reflections will have their frequencies and phase corresponding with the amount of Doppler shift (see Cnaan-On et al. (2015)). Since the sources of movement change their velocity over time, it is usually best to model the signal as a band-limited random $X(t)$ process with spectral content centered around DC.

At the reader input, spread-Doppler reflections will result in

$$r(t) = \sum_{n=-\infty}^{\infty} \sum_{q=1}^{Q} \alpha(r_q) p(t - nT_p - \tau_q) \cdot X_q(t) \tag{4.9}$$

where Q is the number of spread Doppler clutter returns, $\alpha(r_q)$ is the attenuation due to the two-way backscatter path of length r_q, $X_q(t)$ is a random process modeling the Doppler spread reflections and τ_q is the time delay associated with the two-way backscatter path of length r_q.

For CW, after receiver processing,

$$u(t) = r(t) * s^*(t) = \sum_{q=1}^{Q} \alpha(r_q) X_q(t). \tag{4.10}$$

where the random process $X_q(t)$ also absorbs the phase dependent DC contribution $\phi(\tau_q)$.

For pulse train, after receiver processing,

$$u(t) = r(t) * s^*(t) = \sum_{q=1}^{Q} \alpha(r_q) D_q(t - \tau_q) X_q(t) \tag{4.11}$$

Different models have been proposed in the literature for describing the statistics of clutter such as the K-distribution to describe sea clutter (Ward et al. (2006)),

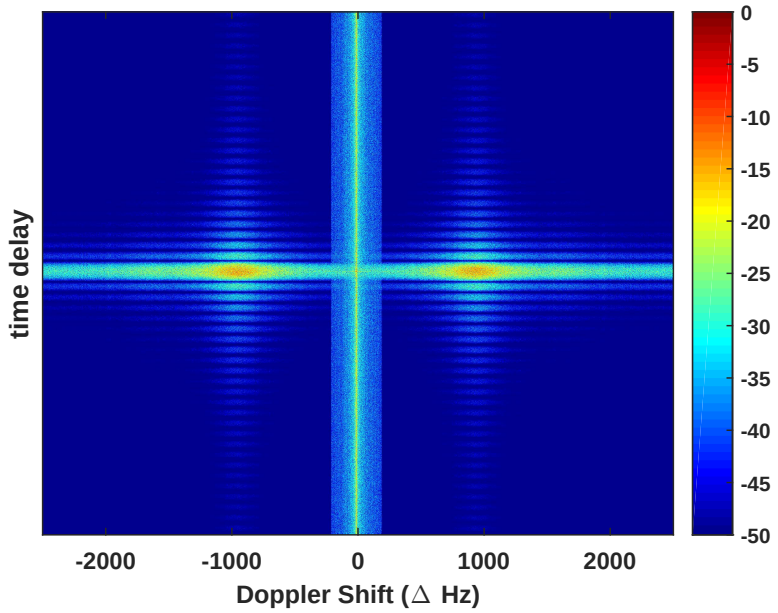


FIGURE 4.3: Delay-Doppler simulation of a signaling RF tag coded with RLL(1,3) across pulses (seen as the symmetric concentrations around $+/-1000$ Hz) and added spread-Doppler clutter (<200 Hz) at arbitrary power (seen as a narrow band around the Doppler DC). The RLL Doppler code shapes the Doppler spectrum of the tag and pushes it away from the clutter. Scale is in dB.

Weibull to describe ground clutter (Sekine et al. (1981)), Rayleigh and others (Blasch (2004)). However, in order to focus on the coding rather on specific clutter modeling, simulations in this work use a simplistic clutter distribution that is inversely proportional to the Doppler frequency $S(f) \propto 1/f_D$.

4.3 Doppler run length limited channel coding

4.3.1 RLL codes overview

RLL coding originated in magnetic recording research with the purpose of limiting the number of magnetic flux changes per given area of the disk in order to avoid hardware limitations or channel impairments. The code manipulates the binary message data to limit the placement of ones in the sequence, which maps to flux flips. Limiting long stretches between ones controls the lower frequency content,

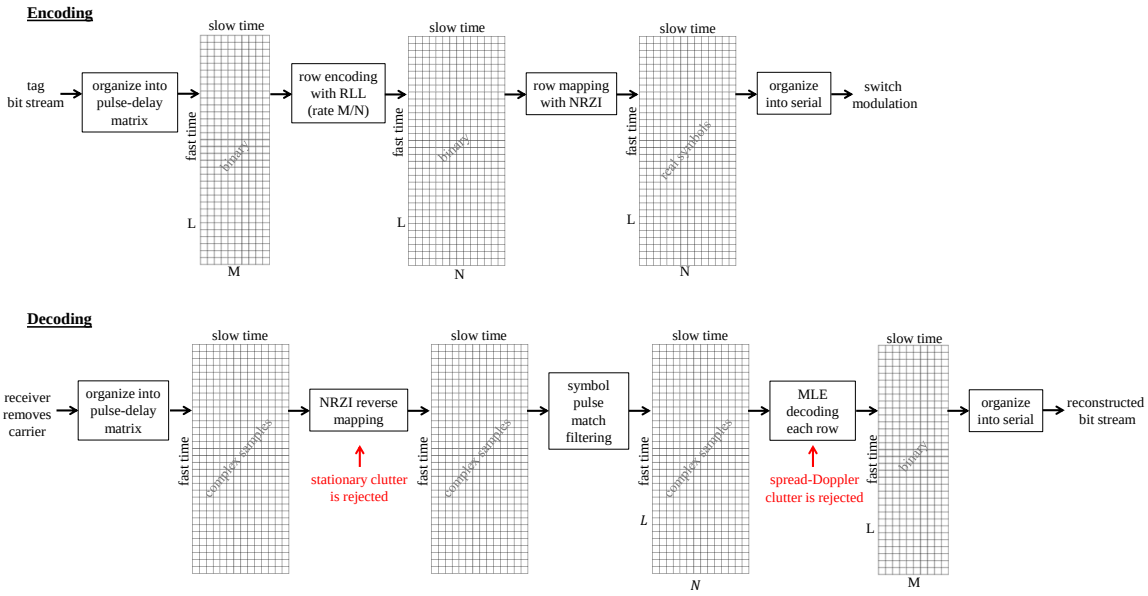


FIGURE 4.4: Run-length limited Doppler encoding and decoding process

while enforcing a minimum distance between ones controls the higher frequency content. This provide a way of shaping of the respective spectrum of the message, which provides resilience to specific channel impairments at the expense of lower data rate. Codes consist of blocks and are defined by four parameters: D,K,M,N, where D is the minimum and K is the maximum number of zeroes between consecutive ones, and M/N is the rate of the code.

4.3.2 Doppler RLL encoding setup

An arbitrary bit stream is broken into blocks, whose length L corresponds with the interrogating pulse duration T_p and the tag symbol duration T_s, such that $L = T_p/T_s$ is an integer number of symbols per pulse and assumed to be a universal system parameter. Choosing L determines effectively the Doppler sampling rate. A higher sampling rate will allow better mitigation of Doppler interference in the lower band near DC.

The blocks are then assembled side by side to create a rectangular matrix whose columns are time and rows are pulse index. Matrix dimensions are: $L \times M$. For

synchronization purposes at the decoder, we mark these $L \cdot M$ bits as a single frame length. The matrix organization is adapted from radar pulse-Doppler signal processing Richards (2005), where the columns are dubbed *fast time* and the rows are *slow time*.

An RLL code with rate M/N is now employed over the *slow-time* rows. Each row is independently encoded and the output is organized into matrix dimensions of: $L \times N$. Note that the coding does not change the number of bits per pulse, hence no change to the hardware symbol rate is needed. The *slow-time* encoding allows the Doppler spectrum manipulation across pulses.

The next step of encoding is using non-return to zero inverted (NRZI) mapping of each row from binary to two level physical symbols, suitable for BPSK constellation modulation. As a differential mapping, a binary one translates into a transition of the physical level, while a binary zero maintain the physical level. The first column relates to the last column from the previous frame to maintain continuity of the differential mapping across pulses. The resulting matrix consists now of symbols rather than binary numbers.

The matrix is then broken into N blocks, each one is a pulse length, and reorganized consecutively into a stream of symbols, which are then fed into the phase modulator.

The above encoding considers a pulse train interrogating signal. However, when a continuous wave is used, rather than a pulse train, the presented framework is still valid by setting $p(t)$ to be equal to an integer number of sinusoid wavelengths, such that notion of a pulse becomes unnecessary.

4.3.3 Doppler RLL decoding setup

The first step for the receiver is to remove the sinusoidal carrier using a conjugate copy of the carrier used for the transmitted signal. The next step is organizing

the received processed signal into the same *fast time-slow-time* matrix structure which was used as the foundation of the encoding process. Each column consists of the processed return duration equivalent to a single pulse and consecutive pulse durations are aligned side by side. It is important to stress that the because of the time-delay and lack of reader-tag synchronization, the matrix will have some shift, such that a return from a transmitted pulse will be shifted and lay in more than one column. This shift, however, does not alter the rows consistency and allow for the rows NRZI reverse mapping.

Next, a reverse mapping of NRZI is performed over the rows. This is done by subtracting each column from the adjacent column, which contains the next pulse duration return (effectively removing the differential NRZI mapping). When considering the first column in a frame, we can use the last column from the previous frame as a reference for subtraction. In addition to the re-mapping, this step effectively also performs Doppler filtering, which is discussed later in subsection 4.3.5. The reverse mapping of NRZI of the processed received signal can be done in the analog domain as well as over the sampled signal. The benefit of doing it in the analog domain is the ability to improve the receiver dynamic range by filtering a lot of the clutter energy, masking the weak signal coming from the tag modulation.

Next the receiver performs the initial processing of removing the waveform coding as described earlier and discussed in details in section 4.2.1.

In the next step, the receiver needs to align the matrix shift such that the tag symbols are aligned into the original frame structure as signalled by the tag. Any conventional method of synchronization to estimate the clock phase ϕ of the tag discussed in section 4.2.1 can be used, such that the tag's symbols are synchronized with the receiver clock and matrix is aligned.

The next step is performing a matched filer for the rectangular symbol pulses $q(t)$ and sampling the output. Then a maximum-likelihood estimation (MLE) decoding

criteria is used to choose among all the relevant RLL codewords on the rows, and infer the respective information bits. The last step is converting the matrix structure back into serial.

4.3.4 Extension to QAM symbols

RLL codes were originally designed for use with a BPSK modulation. A general method of extending RLL codes to QAM modulation is proposed such that for a QAM enabled RF tag it is possible to achieve the Doppler spectrum shaping as described in previous sections for a BPSK RF tag. Starting with 4-QAM constellation formation, we assume two statistically independent data streams x'_n and y'_n. In the suggested framework, this can be achieved for example by taking data from two different frames. After performing the same RLL coding on each stream separately, the outcome is x_n and y_n. After performing NRZI mapping, the discrete Fourier transform of the shaped spectra are

$$X_k = \sum_{n=0}^{(L-1)(N-1)} x_n e^{-2\pi jikn/(LN)} \tag{4.12}$$

and (4.13)

$$Y_k = \sum_{n=0}^{(L-1)(N-1)} y_n e^{-2\pi jikn/(LN)} \tag{4.14}$$

Now, a 4-QAM stream is synthesized by using in-phase (I) and quadrature (Q) constellation mapping, such that a single bit from x_n and a single bit from y_n are mapped together into a single 4-QAM symbol, and see Fig. 4.5

$$z_n = (x_n + jy_n)/2 \tag{4.15}$$

and respectively the frequency magnitude

$$Z_k = \frac{1}{2}(X_k + e^{j\frac{\pi}{2}} Y_k) \tag{4.16}$$

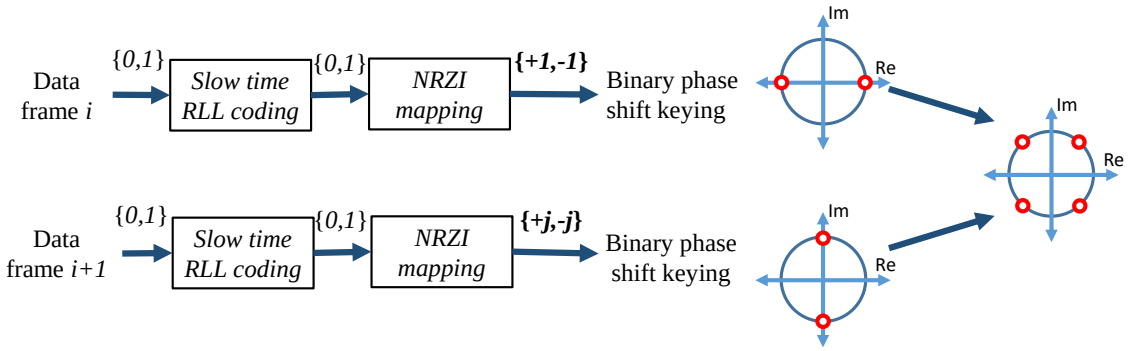


FIGURE 4.5: RLL coding for quadrature phase shift keying modulation.

Given the statistical independence between X_k and Y_k and since we are interested mostly in the spectrum magnitude, we take the expectation with regards to instantiations of X_k and Y_k

$$|E\{Z_k\}| = \frac{1}{2}|E\{X_k + e^{j\frac{\pi}{2}}Y_k\}| = \frac{1}{2}|E\{X_k\} + e^{j\frac{\pi}{2}}E\{Y_k\}| \tag{4.17}$$

$$= \frac{1}{2}|E\{X_k\}| + |E\{Y_k\}| = |E\{X_k\}| \tag{4.18}$$

where the transition is valid only because the expected phase of X_k and Y_k is the similar. The achieved spectrum is equivalent to the spectrum of a single stream. Decoding for 4-QAM RLL is straight forward, and as a first step all 4-QAM symbols are broken into two streams from the in-phase and quadrature.

Once we establish the mechanism of independently encoding the in-phase axis and quadrature axis with 4-QAM RLL, we can turn to using multi-level RLL codes. Instead of using 2-level codes that were used until now, we can employ 4-level or even higher codes (see Schouhamer-Immink (1991)) to support a higher cumulative QAM constellations.

The proposed structure preserves the desired RLL spectrum shaping characteristic for 4-QAM and QAM in general. In QAM the data rate increases on the expense of smaller energy per bit E_b and hence larger error probability, so it is more suitable to high SNR scenarios.

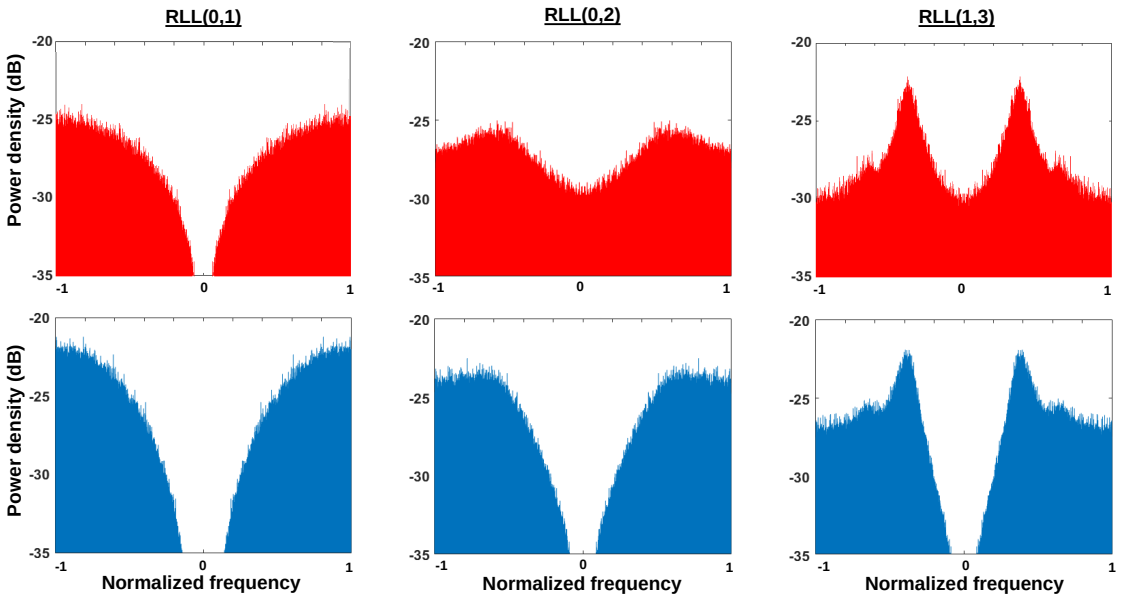


FIGURE 4.6: Spectrum of selected run-length limited codes before (upper row) and after (lower row) the inverse NRZI subtraction operation.

4.3.5 Clutter rejection by using RLL codes

The clutter rejection is accomplished in two layers of the decoding process. The first layer is a result of the reverse mapping of the NRZI. The subtraction of two neighboring pulses inverts the differential mapping but also act as a Doppler spectrum filter. Eventually each point of the received signal is subtracted from a point exactly one pulse duration T_p apart. The resulting filtering effect can be seen in Fig. 4.6. The second layer comes from the run-length limited coding that shapes the Doppler spectrum of the message signal and pushes it outside of the interference domain. A few examples of various RLL codes can be seen in Fig. 4.6. Cumulatively the overall Doppler filter contribution can be seen in Fig. 4.7.

Since focus of this paper is on the coding rather than on specific clutter models, a simplistic statistical model is chosen as described in section 4.2.4. The clutter model used is a mixture of $1:1$ ratio between spread-Doppler and static clutter. The spread Doppler clutter was synthesized by combining 5 random frequency fluctuations for

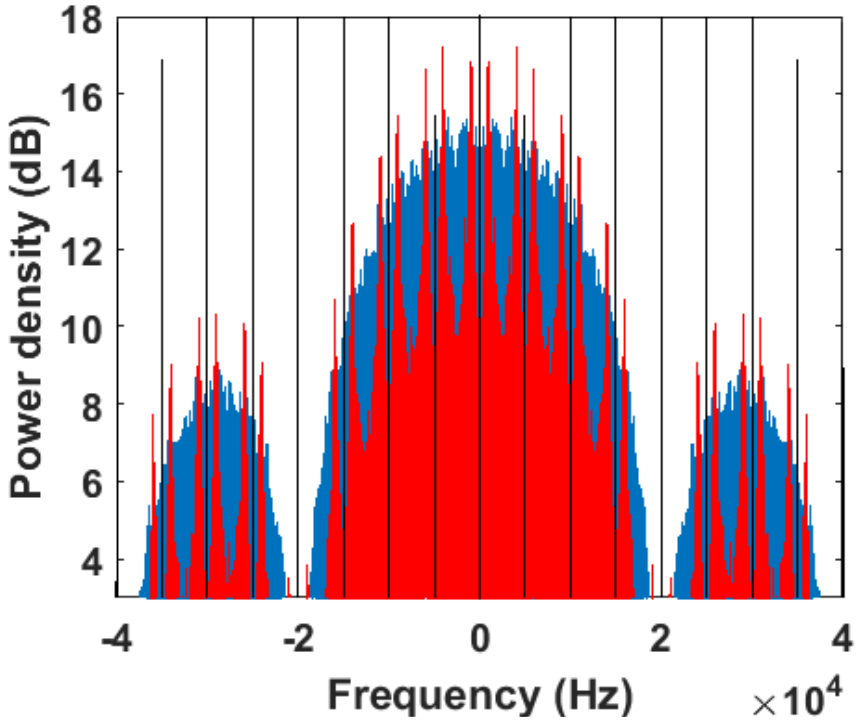


FIGURE 4.7: Spectrum of Doppler run-length limited code $(1, 3)$ driving a rectangular pulse after the inverse NRZI subtraction operation (red). Static clutter returns shows as lines (black). At the back (blue), a reference of uncoded random data with rectangular pulse and no subtraction operation. The coded spectrum exhibits notches that appear at integer multiples of the pulse repetition frequency, where clutter is dominant.

every row of the encoding matrix.

The codes chosen for simulations are: RLL(0,1) with rate 1/2 (effectively this is the FM0 code proposed in the EPC Gen-2 protocol), RLL(1,3) with rate 1/2 (effectively this is the Miller code proposed in the EPC Gen-2 protocol, also known as MFM (modified frequency modulation)), RLL(0,2) with rate 4/5, and an uncoded NRZI mapping for benchmark purposes with rate 1.

Fig. 4.8 shows how different RLL codes compare with changing power level of spread-Doppler interference in the backscatter channel. Note that choosing an RLL code provides a trade-off between interference rejection and data rate. The use of RLL(0,2) with rate 4/5, for example, provides a good balance between a decreased

data rate with better interference rejection. A similar trend can be seen in Fig. 4.9, this time comparing different RLL codes with the spread-Doppler bandwidth of interference.

Fig. 4.10 gives a visual understanding regarding clutter-to-noise ratio. As can be seen, the suggested algorithm is sensitive to the power level of the clutter independently from the noise power levels. In other words, the bit error rate is not the same for similar clutter-to-noise ratio (CNR), but rather depends independently on the amount of clutter and the amount of noise.

To sum, the analysis shows that code rates of 1 and 4/5 are achievable when dealing with low spread Doppler channels, which is an improvement over the current rate 1/2 with current CW mainstream backscatter communication (as it is defined in EPC Gen-2 protocol). For pulse train interrogation waveform, the use of RLL codes can achieve robustness to spread-Doppler clutter, as oppose to the current method that considered only static clutter.

4.4 Waveform coding for high resolution range estimation

The process of ranging is done seamlessly and simultaneously with the communication. Ranging processing is done on a processing branch parallel to communication processing branch. The communication processing is dependent upon the time-delay estimation in order to decode the waveform range coding (if used) and recover the tag symbols. See Fig. 4.2 for detailed processing chain. For CW interrogation signals, time delay estimation is not required, since there is no range code to decode and the tag symbols are readily available for the communication processing.

Ranging can be performed continuously and the time-delay information can be constantly passed to the communication branch. For an application where the tag location is changing unexpectedly, this allows a seamless continuous uninterrupted communication from the tag. However, this work does not handle tags that have

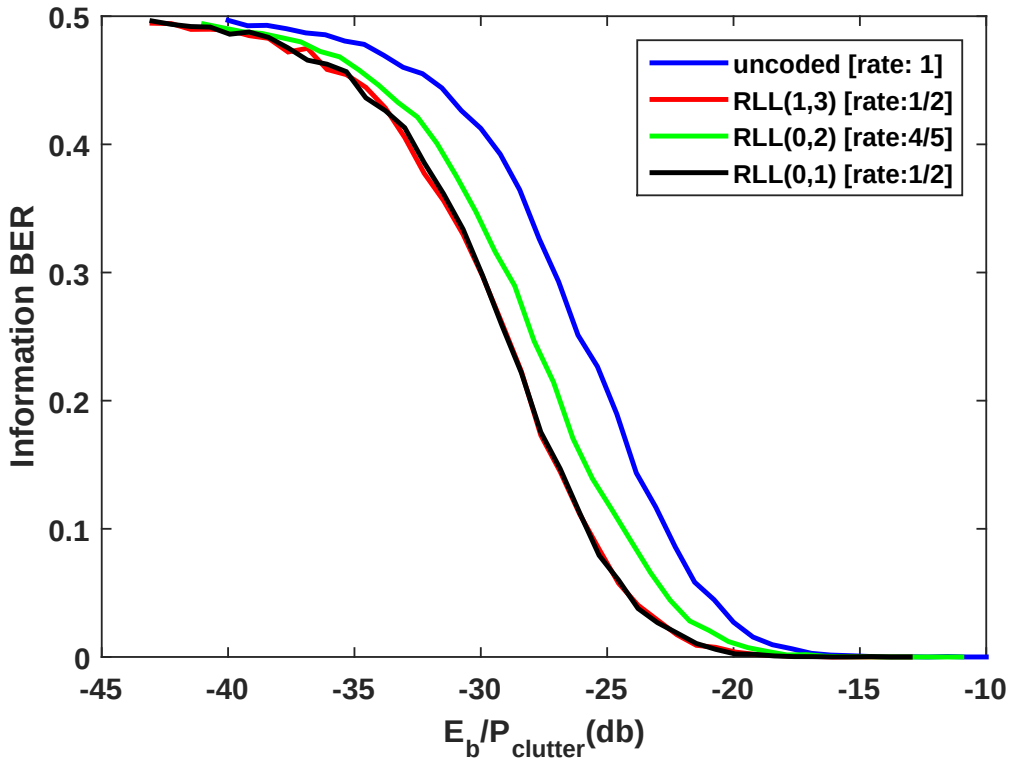


FIGURE 4.8: figure

A comparison of robustness to spread-Doppler self-interference power of various RLL codes. Simulation parameters: averaged over 2000 iterations, clutter model is composed of $1:1$ energy ratio of static and spread-Doppler, clutter bandwidth is < 5 Hz, no noise added.

non-negligible Doppler effect, which is a result of longitudinal velocity with respect to the reader.

For the initial step, where range is unknown, data stream can be still recovered with no data loss; The receiver records the sampled signal for the duration it takes for time delay estimation processing. Then, it can re-feed the samples and start process the communication with the correct time-delay.

4.4.1 Waveform coding and time-delay estimation setup

Waveform encoding is straightforward, as the sinusoidal carrier is modulated according to the chosen phase or frequency code.

At the receiver, the first two steps are identical to those described in the com-

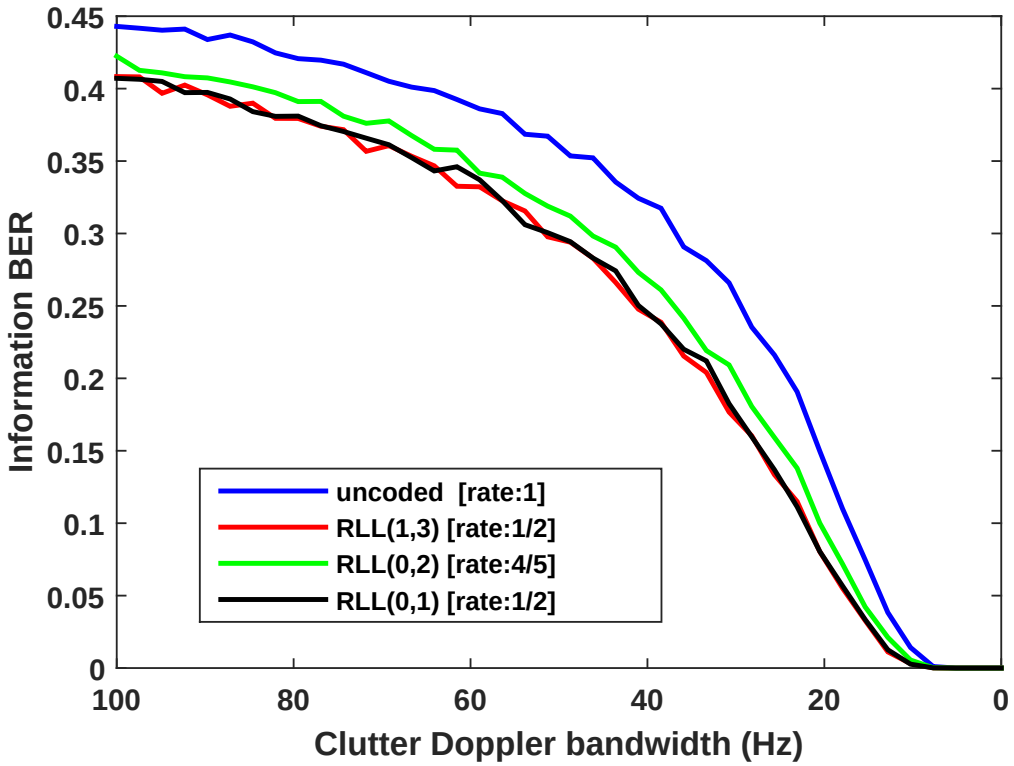


FIGURE 4.9: A comparison of robustness to spread-Doppler self-interference bandwidth of various RLL codes. Simulation parameters: averaged over 5000 iterations, clutter model is composed of $1:1$ energy ratio of static and spread-Doppler, $E_s/P_{clutter} = -20$ dB, no noise added.

munication processing (see section 4.3.3): The sinusoidal carrier is removed using a conjugate copy of the carrier used for the transmitted signal. Then the received signal is subtracted from a delayed copy of itself exactly one pulse duration apart T_p using an analog delay-line. Alternatively, this step can be done digitally but with limited receiver dynamic range because of sampling the strong clutter along with the tag relatively weak signal.

Next, time-delay estimation is performed based on cross-correlation between the reader's transmitted interrogation signal and the backscattered signal from the RF tag. Time-delay is estimated by choosing maximum likelihood or the time-delay associated with the peak of the cross-correlation output.

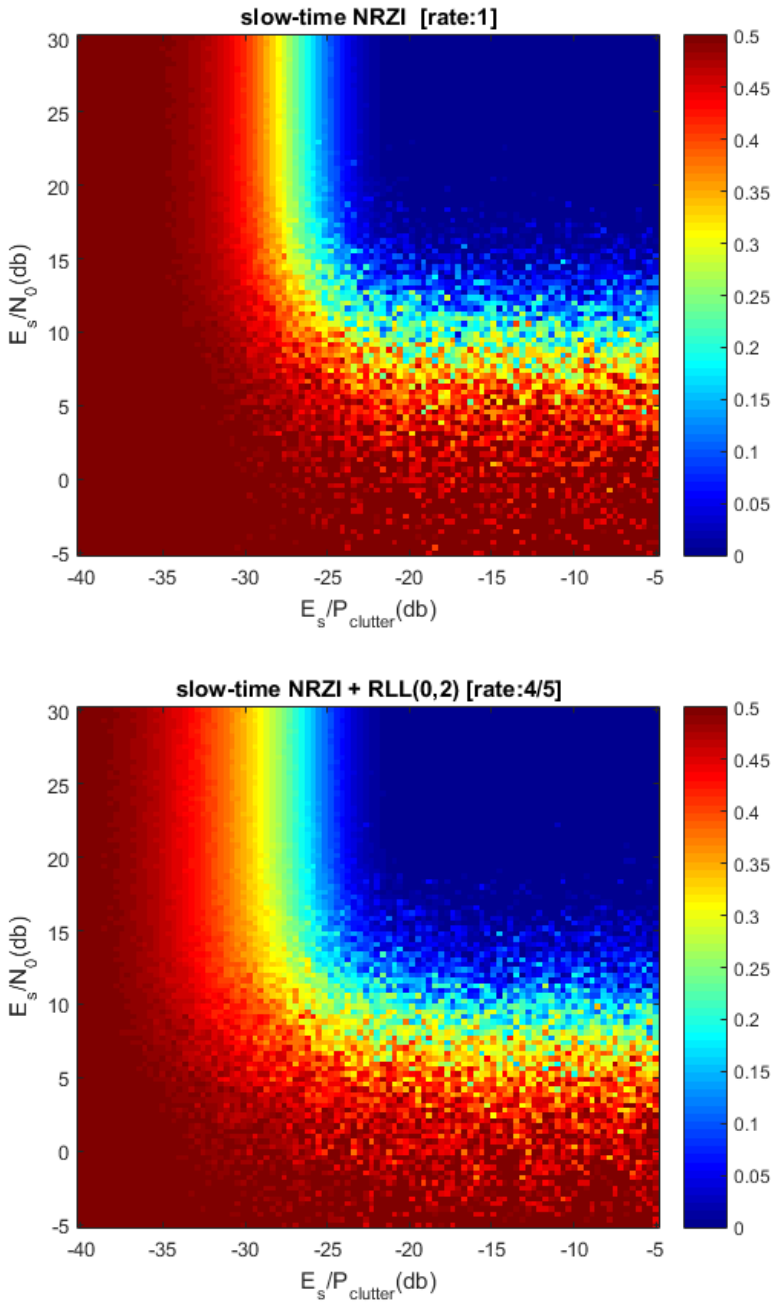


FIGURE 4.10: A comparison of robustness to spread-Doppler self-interference clutter together with additive white Gaussian noise. Z-axis represents the BER. Simulation parameters: averaged over 100 iterations, clutter model is composed of $1:1$ energy ratio of static and spread-Doppler,clutter bandwidth is < 5 Hz.

Once time-delay is estimated, the receiver demodulates the waveform code from the received signal with the correct time-delay shift. After that step, the signal

contains the tag modulation and can be processed further to extract the tag message (sec. 4.3.3).

Conversion from time-delay to range is straightforward as it is based on the linear transformation between time-delay and range $r = c \cdot \tau/2$, where c is speed of light and τ is the two-way time delay from the tag. This work will use the terms time-delay estimation and ranging interchangeably, while they are effectively equivalent in the scope of this work.

4.4.2 Time-delay estimation analysis

Radar signal design theory studies different waveform codes with respect to their ability to estimate time-delay given parameters such as coherence time, Rayleigh resolution, peak sidelobe level and Doppler resilience. The ambiguity function is the standard tool that is used for such evaluation (see Levanon and Mozeson (2004)). From a system design perspective, the choice of the reader's interrogation waveform can determine desired range estimation properties, for example prioritizing resolution over peak sidelobe level.

Naturally, longer coherence time (i.e. more pulses in the correlated pulse train) will perform well against random noise that is averaged over many pulses, or random modulation from tag (as discussed later in following sections). However, longer coherence time also needs to take into account drifts in tag clock ϕ and movement of the tag that can cause errors in the time-delay estimation.

By using continuous pulse train, the time-delay estimation is limited by the ability to distinguish between returns coming from different pulses. The resulting ambiguity is between time-delays that are with integer additions of the pulse duration T_p. An unambiguous time-delay estimation is achievable if the time-delay is bounded by $-T_p/2 \leqslant \hat{\tau} \leqslant T_p/2$. As seen, the choice of T_p is key to determine the unambiguous range and should be considered to suite a specific use case. Translation into unam-

biguous range yields $-\frac{cT_p}{4} \leqslant \hat{r} \leqslant \frac{cT_p}{4}$, where c is the speed of light. For example, a pulse repetition frequency (PRF) of 5 Khz (or T_p of 200 μsec) gives an unambiguous range of 15 Km, which is suitable for certainly indoor and other mid-range use cases.

4.4.3 The effect of tag modulation on time-delay estimation

Two aspects make time-delay estimation in backscatter communication unique. First, the tag modulation alters the backscattered signal, thus distorting the interrogation waveform code besides the usual time-delay and Doppler shift. Second, implementing a key part of the clutter filtering at the receiver front end (i.e. pulse subtraction or NRZI reverse mapping) is causing phase mirror impairment that is also impacting the reflected waveform signal. To demonstrate that, examine the subtraction of two unit circle complex numbers that each represents some PSK constellation point, e.g. BPSK with alphabet $\{e^0, e^{j\pi}\}$.

$$r = e^{jx_1} - e^{jx_2} = e^{jx_1} + e^{j(x_2+\pi)} \tag{4.19}$$

Then the outcome of that term can take the following values

$$r = \begin{cases} 2e^0 & \text{if } x_1 = 0 \text{ and } x_2 = \pi \\ 2e^{j\pi} & \text{if } x_1 = \pi \text{ and } x_2 = 0 \\ 0 & \text{if } x_1 = \pi \text{ and } x_2 = \pi \\ 0 & \text{if } x_1 = 0 \text{ and } x_2 = 0 \end{cases} \tag{4.20}$$

As one can see, some resulting phase terms contribute a $e^{j\pi}$ phase rotation (or mirroring) to the envelope signal that is mixed with. Phase contribution of e^0 would be transparent to the envelope signal and the two other contributions will zero the envelope signal. Assuming a uniformly distributed random bit stream, the amount of phase-mirrored samples would be 25%.

Now, we apply this mathematical analysis to the time-delay estimation problem. We start by examining the phase term of a received signal right after the subtraction operation at the receiver front end. We assume a BPSK reader interrogation range

code (such as a Barker code) and a BPSK modulating tag. The phase of the received signal is affected by: τ_m - time-delay modulo the sinusoidal carrier wave period and ϕ - tag - Reader clock phase difference. Both are assumed to be constant (time invariant) unknowns during the processing duration.

$$e^{jz}e^{j\tau_m}\left[e^{j\phi}(e^{jy_1} - e^{jy_2})\right] = e^{jz}(e^{jy_1} + e^{jy_2+\pi})e^{j(\tau_m+\phi)} \tag{4.21}$$

where e^{jz} is the reader waveform code phase, $e^{j\tau_m}$ is the phase contribution from the time-delay modulo wavelength of the sinusoidal carrier, $e^{j\phi}$ is tag - Reader clock phase difference contribution, and e^{jy} is the tag BPSK phase modulation, taking phase values of 0 or π.

As we collect terms, it is possible to see that $e^{\tau_m+\phi}$ can be corrected by a standard procedure of constellation rotation (see Thomas et al. (2012)). However by examining the term $e^{jz}(e^{jy_1} + e^{jy_2+\pi})$ one can see that a π phase shift can be contributed to either a waveform phase code change $z = \pi$ or from the tag symbols phase flip e.g. $y_1 = \pi, y_2 = 0$. This creates an ambiguity about the cause of the phase flip, so the reader cannot distinguish if it is a result of the tag modulation (and be reverted) or the range coded waveform (and then it is needed for desired cross-correlation). Cross-correlation with such modulated distorted signal ends up with poor results and see Fig. 4.11. In following sections we show that for some combinations of reader waveform code and tag modulations, this ambiguity can be resolved and the waveform code z can be reconstructed to yield the desired cross-correlation.

4.4.4 Frequency waveform coded interrogation signals

We now consider two types of frequency modulated range coding: linear frequency modulation (LFM) and Costas coding.

LFM is composed of a continuous phase signal sweep in frequency over some

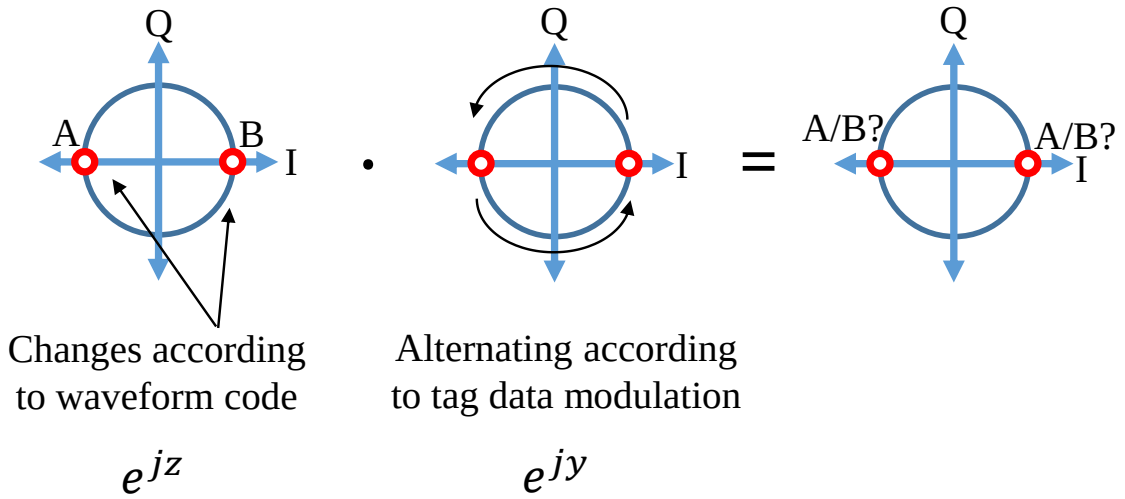


FIGURE 4.11: Symbols constellation demonstrates a phase mirror impairment. The phase ambiguity is caused when a reader waveform code is using a bi-phase phase shift-keying (BPSK) and RF tag is using BPSK as well.

bandwidth B. A single pulse is describes as

$$u(t) = \frac{1}{\sqrt{T_p}}\Pi(\frac{t}{T_p})exp(j\pi\frac{B}{T_p}t^2) \tag{4.22}$$

where $\Pi(t)$ is the rectangular function defined as

$$\Pi(t) = \begin{cases} 0 & \text{if } t \leqslant -\frac{1}{2} \\ 1 & \text{if } -\frac{1}{2} \geqslant t \leqslant \frac{1}{2} \\ 0 & \text{if } t \geqslant \frac{1}{2} \end{cases} \tag{4.23}$$

Costas coded pulse is a set of M discrete frequencies that are sent according to some order a, single frequency at a time for a chip duration t_b ($T_p = M \cdot t_b$). A single pulse of Costas can be described as Levanon and Mozeson (2004)

$$a = \{a_1, a_2, .., a_M\} \tag{4.24}$$

$$u(t) = \frac{1}{sqrt(Mt_b)}\sum_{m=1}^{M} u_M[t-(m-1)t_b] \tag{4.25}$$

$$\text{where } u_m(t) = \begin{cases} exp(j2\pi\frac{a_m}{t_b}t), & 0 \leqslant t \leqslant t_b \\ 0, & elsewhere \end{cases} \tag{4.26}$$

Unlike phase codes (as Barker or Golomb) that contain a discrete set of phases, frequency modulated codes are made of a collection of frequencies with mostly a continuous phase. The tag bi-phase modulation signal causes abrupt phase flips of π that are destructive to discrete phase waveform code (see sec. 4.4.3), but do not change in nature the continuous phase frequencies that constitute the frequency modulated code.

We turn to examine the effect of tag modulation on Costas code. The reader is sending frequencies from $\{e^{j2\pi\theta_1 t}, \ldots, e^{j2\pi\theta_M t}\}$ and a BPSK tag is modulating with symbols from alphabet $\{e^0, e^{j\pi}\}$. The phase of the received signal after the pulse subtraction operation at the receiver front end is similar to the term in eq. 4.21. The difference is that now the term e^{jz} is not a discrete phase, but rather a time varying phase. Two consecutive time samples t_1 and t_2 are considered.

We assume a π phase jump in the sampled signal between t_1 and t_2, caused by the subtraction between two tag symbols (e.g. $y_1 = \pi, y_2 = 0$). As a result, from t_2 onwards the phase term will have an addition of π. Detailing the phase terms $\zeta(t)$ at time samples before and after the phase jump:

$$\begin{aligned}
\zeta(t_0) &= 2\pi\theta t_0 \\
\zeta(t_1) &= 2\pi\theta t_1 \\
\zeta(t_2) &= 2\pi\theta t_2 + \pi \\
\zeta(t_3) &= 2\pi\theta t_3 + \pi
\end{aligned}$$

Taking the instantaneous angular frequency defined as $\omega(t_n) = \frac{\zeta_n - \zeta_{n-1}}{t_n - t_{n-1}}(t_n)$:

$$\begin{aligned}
\omega(t_1) &= 2\pi\theta \\
\omega(t_2) &= 2\pi\theta + \pi Fs \\
\omega(t_3) &= 2\pi\theta
\end{aligned}$$

we observe that we have a frequency discontinuity at t_2.

Now, instead of integrating back, we reconstruct the phase by multiplying with time variable t

$$\omega(t_1) \cdot t_1 = 2\pi f t_1$$
$$\omega(t_2) \cdot t_2 = 2\pi f t_2 + \pi F_s t_2$$
$$\omega(t_3) \cdot t_3 = 2\pi f t_3$$

where F_s is the receiver sampling rate.

The result is the original Costas signal when we removed the ongoing π phase additions. Where a phase jump was, there will be now only a single sample with signal discontinuity $\pi F s t$, and all following samples onwards would not have that π phase addition. Examining the phase discontinuity term a bit further shows that it will contribute phase terms of π for odd samples, or 2π for even samples. On average this means that in 50% of cases, the phase discontinuity amounts to actually a continuity. On the other 50% these samples will cause some degree of degradation in the cross-correlation.

We now turn to examine the cross-correlation overall term for all tag modulation combinations. As shown in eq. 4.20, for modulation values of $y_1 = \pi, y_2 = 0$, the term contribution value will be $2e^0$. For modulation values of $y_1 = 0, y_2 = \pi$, after phase reconstruction as described, the term contribution value will also be $2e^0$ (with discontinuities handles separately at the end), and for modulation values of $y_1 = y_2$, after phase reconstruction, the term contribution value will be 0. We assume y_i are independent and identically distributed random variables with values taken from BPSK constellation of $\{e^0, e^{j\pi}\}$, hence we define $r'_m = (e^{jy_1} + e^{jy_2+\pi})$ with respective values

$$r'_m = \begin{cases} 2 & \text{with prob.= } 1/2 \\ 0 & \text{with prob.= } 1/2 \end{cases} \tag{4.27}$$

So, it is possible to express the processed signal as

$$g(t) = r'_m(t) \cdot s(t - \tau) \tag{4.28}$$

where $s(t)$ is the transmitted interrogation signal, r'_m is the phase term contribution from tag modulation after pulse subtraction at the front end and phase reconstruction.

We now turn to examining the time-delay estimation with the reconstructed waveform. We consider the cross-correlation of coherent pulse train. In that case it is justified to look at the expected value of the cross-correlation when the number of coherent pulses is large enough. Expectation is taken with respect to the random tag modulation

$$\mathbb{E}\{(s(t') \star g(t'))(t)\} = \mathbb{E}\{\sum_{m=-\infty}^{\infty} s^*(t')g(t'+t)\} \tag{4.29}$$

$$= \sum_{m=-\infty}^{\infty} s^*(t')s(t'-\tau+t)\mathbb{E}\{r'(t'+t)\} \tag{4.30}$$

$$= \sum_{m=-\infty}^{\infty} s^*(t')s(t'-\tau+t)(\frac{1}{2}\cdot 2 + \frac{1}{2}\cdot 0) \tag{4.31}$$

$$= (f \star g)(t) \tag{4.32}$$

where $\star$ stands for the cross-correlation

The result shows that the cross-correlation with the reconstructed waveform is in general equivalent to the cross-correlation of an unmodulated coded waveform. We now turn to examine the effect of the discontinuities described earlier on the cross-correlation. Consider a modulating tag with symbol rate of M symbols per pulse and $F_s \cdot T_p$ samples per pulse. Our analysis in eq. 4.20 shows that on average only 25% of samples contribute phase mirroring, and 50% of those will contribute π after our phase reconstruction processing as explained. Consequently the ratio of distorted samples per pulse out of all samples per pulse is:

$$\frac{.5 \cdot .25 \cdot M}{F_s \cdot T_p} \tag{4.33}$$

For example, a choice of $M = 500$, pulse reptetiton freq.$= \frac{1}{T_p} = 5\ Khz$, $F_s = 20\ Mhz$ gives a ratio of distorted cross-correlation samples of 3% which is relatively low number.

The same mathematical derivation also applies to LFM waveform coding, with similar results. When comparing previous methods of ranging with LFM, the method described by Carlowitz et al. (2013) does not have unknown tag modulation effect. This is achieved by using coding that trades data rate (1/2 code rate) with signal energy concentrated at the range induced carrier. The amount of energy used for ranging is therefore 50% of the signal. With the method proposed above, up to the entire signal energy can be used for the purpose of ranging, which translate to 3 dB increas in SNR terms of available energy for range estimation.

4.4.5 Asymmetric bi-phase waveform coded interrogation signals

Now, we examine another category of reader-tag codes combinations that can overcome the phase mirror impairment caused from tag modulation. Consider an asymmetric bi-phase $\{e^0, e^{j\theta}\}$ reader interrogation waveform code (such as a Golomb code) and a BPSK modulating tag $\{e^0, e^{j\pi}\}$. The phase of the received signal after the subtraction operation at the receiver front end is similar to the term in eq. 4.21. Similarly, the term $e^{\tau_m+\phi}$ can be corrected as suggested before. By examining the term $e^{jz}(e^{jy_1} + e^{jy_2+\pi})$ one can see now that a π phase shift is only attributed to a tag symbols phase flip e.g. $y_1 = \pi, y_2 = 0$. Waveform phase code change of z are asymmetric and will result in θ or $\pi - \theta$ phase shifts.

As can be seen in Fig. 4.12, the phase mirroring adds two more constellation points that are exactly mirrored of the original constellation points. The analysis for this case, as oppose to the phase mirroring in section 4.4.3, shows that the constellation ambiguity is resolvable. The receiver can distinguish if the cause of the phase flip is a result of the tag modulation or the waveform code by leveraging the

asymmetry of the waveform code against the phase mirroring. Next, the receiver can remap the lower half plane of the constellation (between $\pi - \frac{\theta}{2}$ and $2\pi - \frac{\theta}{2}$) to correct for the random tag modulation phase mirroring effect. This is done by π rotation of only the lower half plane.

As shown in eq. 4.20, for modulation values of $y_1 \neq y_2$, after remapping, the term contribution value will be $2e^0$, for modulation values of $y_1 = y_2$, after remapping, the term contribution value will be 0. We assume y_i are independent and identically distributed random variables with values taken from BPSK constellation of $\{e^0, e^{j\pi}\}$, hence we define $r'_m = (e^{jy_1} + e^{jy_2+\pi})$ with respective values

$$r'_m = \begin{cases} 2 & \text{with prob.= } 1/2 \\ 0 & \text{with prob.= } 1/2 \end{cases} \tag{4.34}$$

So, it is possible to express the processed signal as

$$g(t) = r'_m(t) \cdot s(t - \tau) \tag{4.35}$$

where $s(t)$ is the transmitted interrogation signal r'_m is the phase term contribution from tag modulation after pulse subtraction at the front end and constellation remapping.

We now turn to examining the time-delay estimation with the reconstructed/remapped waveform. We consider the cross-correlation of coherent pulse train. In that case it is justified to look at the expected value of the cross-correlation when the number of coherent pulses is large enough. Expectation is taken with respect to the random

tag modulation

$$\mathbb{E}\{(s(t') \star g(t'))(t)\} = \mathbb{E}\{\sum_{m=-\infty}^{\infty} s^*(t')g(t'+t)\} \tag{4.36}$$

$$= \sum_{m=-\infty}^{\infty} s^*(t')s(t'-\tau+t]\mathbb{E}\{r(t'+t)\} \tag{4.37}$$

$$= \sum_{m=-\infty}^{\infty} s^*(t')s(t'-\tau+t)(\frac{1}{2}\cdot 2 + \frac{1}{2}\cdot 0) \tag{4.38}$$

$$= (f \star g)(t) \tag{4.39}$$

where $\star$ stands for the cross-correlation

In sum, the remapping is able to reconstruct the waveform coded signal and completely revert the tag modulation. This re-mapping of the constellation however comes with a trade-off. When noise is involved, the receiver might make the wrong re-mapping decision and cause a specific sample point to be mistakenly π phase rotated from its correct location. This can be seen in Fig. 4.13 as the half plane rotation threshold can be easily seen and reveal noisy samples that were mistakenly π rotated. This phenomenon is more pronounced as the two constellation points are closer to symmetry, coming into complete in-resolvability as seen with reader symmetric BPSK as discussed earlier in section 4.4.3.

Consequently, the ability to use Golomb code rather than previously used LFM has the benefit of reduced range sidelobes. For LFM the sidelobes are -13.5 dB lower than the main lobe, where in Golomb, optimal zero sidelobes are achieved (see Levanon and Mozeson (2004)).

4.4.6 Symmetric bi-phase waveform coded interrogation signals

We have seen that in backscatter communication clutter needs to be filtered first, before range estimation or communication can be done. If the tag simply signals a constant symbol, it will be filtered as it cannot be distinguished from the clutter.

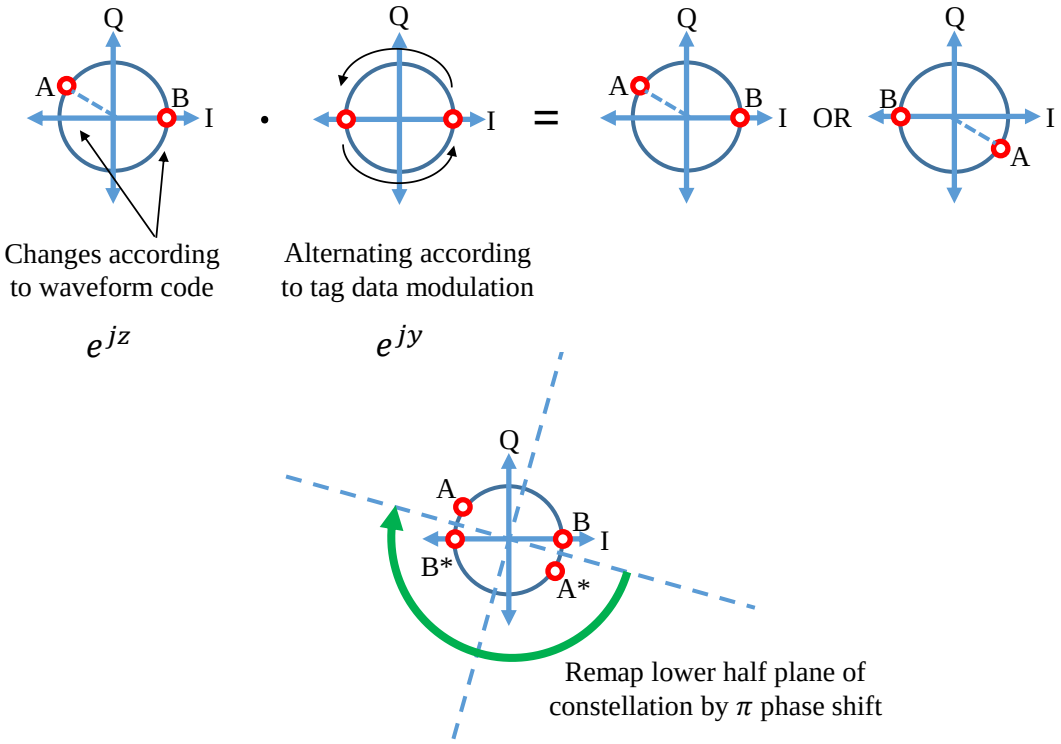


FIGURE 4.12: Symbols constellation demonstrates a phase mirror impairment. The phase ambiguity is resolvable when a reader waveform code is using a asymmetric bi-phase phase shift-keying (BPSK) and RF tag is using BPSK.

Therefore, the tag needs to signal some dynamic time-varying sequence. We have seen however, that for a BPSK reader waveform code, a BPSK tag modulation causes phase mirroring (see sec. 4.4.3).

We propose a quasi-cooperative code that will allow the receiver to reconstruct the range coded waveform for cross-correlation. The coding method leverages quadrature tag modulation and tag data rate. When the tag signals a quasi-cooperative sequence, it comes on the expense of data that could have been signaled instead. We propose to use time division sharing to allow trade-off between data rate and the cooperative range coding. We use the term 'quasi' as we assume the tag is not synchronized with the reader and only knows the reader pulse duration T_p. The reader knows respectively the tag modulation scheme.

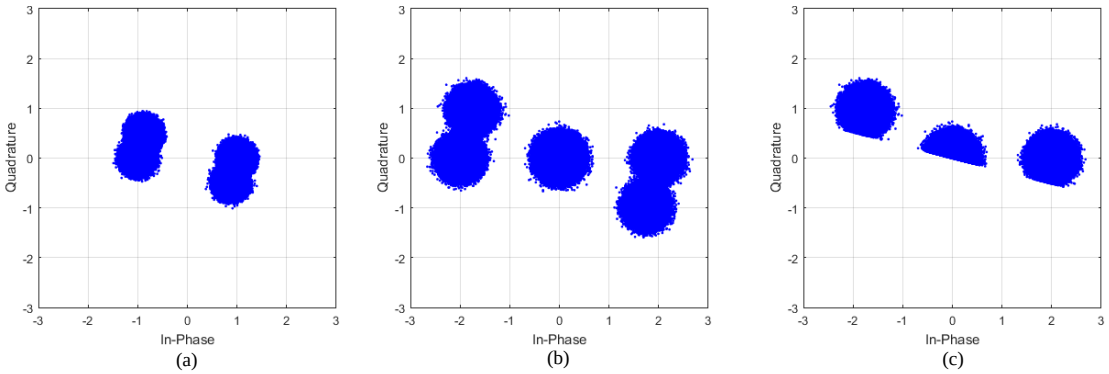


FIGURE 4.13: Simulation results of phase remapping for reader waveform using a asymmetric bi-phase phase shift-keying (BPSK) Golomb15 code and RF tag is using BPSK and random i.i.d symbols modulation. Additive white Gaussian noise at SNR=30 dB. (a) Before receiver front end subtraction (b) After subtraction, notice the increase of noise variance due to the subtraction operation. (c) After receiver remapping.

Quasi-cooperative coding for time-delay estimation

The reader transmits BPSK coded waveforms. The tag signals a quasi-cooperative sequence such that after the front end pulse subtraction at the receiver, the original waveform coded pulses could be reconstructed.

A natural candidate for such a sequence that comes in mind for BPSK tags symbols is the following alternating sequence

$$\underbrace{(-1,-1,..,-1)}_{M},\underbrace{(+1,+1,..,+1)}_{M},\underbrace{(-1,-1,..,-1)}_{M},... \tag{4.40}$$

where M is the number of symbols contained in a reader pulse. After the front end subtraction, the output is the waveform code with some π phase rotation that happens exactly at the tag time-delay during the pulse. This is a result of phase mirroring when the tag changes symbols from pulse to pulse. This only happens once in every pulse, compared with multiple phase flips that happens when the tag signals a random modulation (see sec. 4.4.3). However, even this single phase flip per pulse would still deteriorates the cross-correlation outcome. So, a key difference

in the proposed method is that the waveform code is reconstructed without phase flip.

Now, for the proposed method, a tag with quadrature phase symbols signals the following sequence

$$\underbrace{(-j,-j,..,-j)}_{M},\underbrace{(-1,-1,..,-1)}_{M},\underbrace{(+j,+j,..,+j)}_{M}, \tag{4.41}$$

$$\underbrace{(+1,+1,..,+1)}_{M},\underbrace{(-j,-j,..,-j)}_{M}... \tag{4.42}$$

This sequence would generate a $\frac{\pi}{2}$ phase shift from pulse to pulse, which creates a stepped frequency modulation that would allow it to be distinguished from the BPSK reader modulation.

The receiver has a front end pulse subtraction operation. Then the receiver performs a complementary processing step to the tag sequence by taking a continuous $\frac{\pi}{2}$ half complex plane rotation from pulse to pulse following the processing pattern of

$$Re\{\cdot\}, -Im\{\cdot\}, -Re\{\cdot\}, Im\{\cdot\}, Re\{\cdot\}, \ldots \tag{4.43}$$

The output is the desired reconstructed range coded waveform without any phase mirror impairments, that will yield the desired cross-correlation. A visual step-by-step timing diagram can be seen in Fig. 4.14 that follows the receiver processing of such a quasi-cooperative sequence sent by a QPSK tag. One consideration is that the complementary processing step produces 4-way ambiguity: The $\frac{\pi}{2}$ rotation at the receiver can be rotating forward or backward and take the plus or minus sign. This can be resolved by taking all 4 options and pick the highest peak from the cross-correlation output.

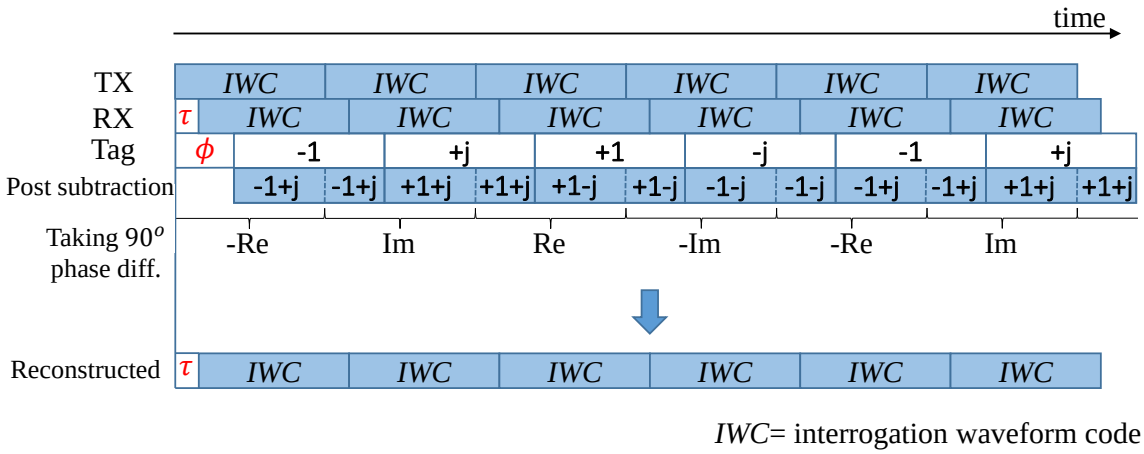


FIGURE 4.14: Time diagram of the signals at the receiver. The receiver has uncertainty in time-delay τ and symbol phase ϕ, yet after processing the waveform code is reconstructed.

Quasi-cooperative coding - data trade-off

At the receiver, a correlation with the transmitted range code allows time-delay estimation, hence ranging. Time sharing ratio of data pulses and quasi-cooperative range code pulses allows a trade-off between information rate and ranging error. The higher the ratio of quasi-cooperative range code pulses sent, the better would be the time-delay estimation. But this comes on the expense of less data pulses signaled. Fig. 4.15 shows the time sharing concept with interleaved data and quasi-cooperative ranging sequences.

Now we consider the cross-correlation output of a pulse train with total of N pulses, where pN of them are mixed with quasi-cooperative range coded tag modulation and $(1-p)N$ are mixed with random data tag modulation, where $0 \leqslant p \leqslant 1$. Considering the cross-correlation at zero delay, we can observe the contribution from the pN pulses that are mixed with quasi-cooperative range code tag modulation and the $(1-p)N$ pulses that are mixed with random data tag modulation. For the pN pulses we effectively have the coded waveform, without distortions. The

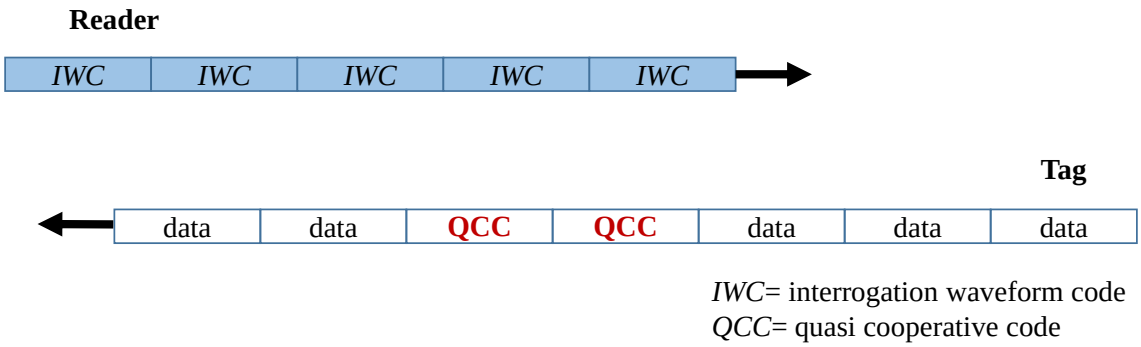


FIGURE 4.15: RF-tag embeds quasi-cooperative code sequences into data stream, and allows time-sharing between data and ranging support sequences.

expected contribution for the cross-correlation is $pNTp$. For the $(1-p)N$ pulses we effectively have the coded waveform that are heavily affected by the phase mirroring impairment. The expected contribution over independent and identically distributed random tag symbols for the cross-correlation is 0 for large number of N, that follows from averaging the outcome of eq. 4.20. Thus, the total contribution is attributed to the quasi-cooperative coded pulses only.

Waveform code with non-optimal periodic autocorrelation

When considering ranging, the autocorrelation function (ACF) of the chosen interrogation waveform code will determine the ranging performance. However, for pulse trains there is a correlation interaction between neighboring pulses, so the periodic autocorrelation function (PACF) is used instead. Some codes have desired ACF but the PACF does not maintain those desired properties (e.g. Barker code). For these codes, when the reader is interested in performing ranging, it can insert blank pulses in between the range code, such that the autocorrelation of a pulse train will yield the desired ACF. This however comes with a trade-off, during that ranging interrogation

period, the blank pulses will not be able to carry back the tag modulation, which translates into half of the data coming from the tag lost. It is possible to overcome this loss if we consider adding redundancy in the tag messages modulation. After time-delay is estimated, the reader continues to work with regular pulse train (no blanks), since now the range code is merely a modulation that the reader can undo with the time-delay estimation and be left with the tag symbols.

4.4.7 Ranging with frequency and phase coded interrogation signals - simulation results

Simulation results in Fig. 4.16 demonstrate the difference between combination of waveform code and tag modulation. Simulation used SNR of 0 dB with 4000 processed pulses in a pulse-train, 4000 symbols per pulse and averaged over 100 iterations. As expected Costas coding and Golomb coding with remapping/reconstructing receiver performs well with tag random phase modulation. Barker code requires some minimum ratio of quasi-cooperative pulses in order to maintain good time-delay estimation.

Simulation results in Fig. 4.17 demonstrate the difference between combination of waveform code and tag modulation. Simulation used with 4000 processed pulses in a pulse-train, 4000 symbols per pulse, 99% of data utilization and averaged over 100 iterations.

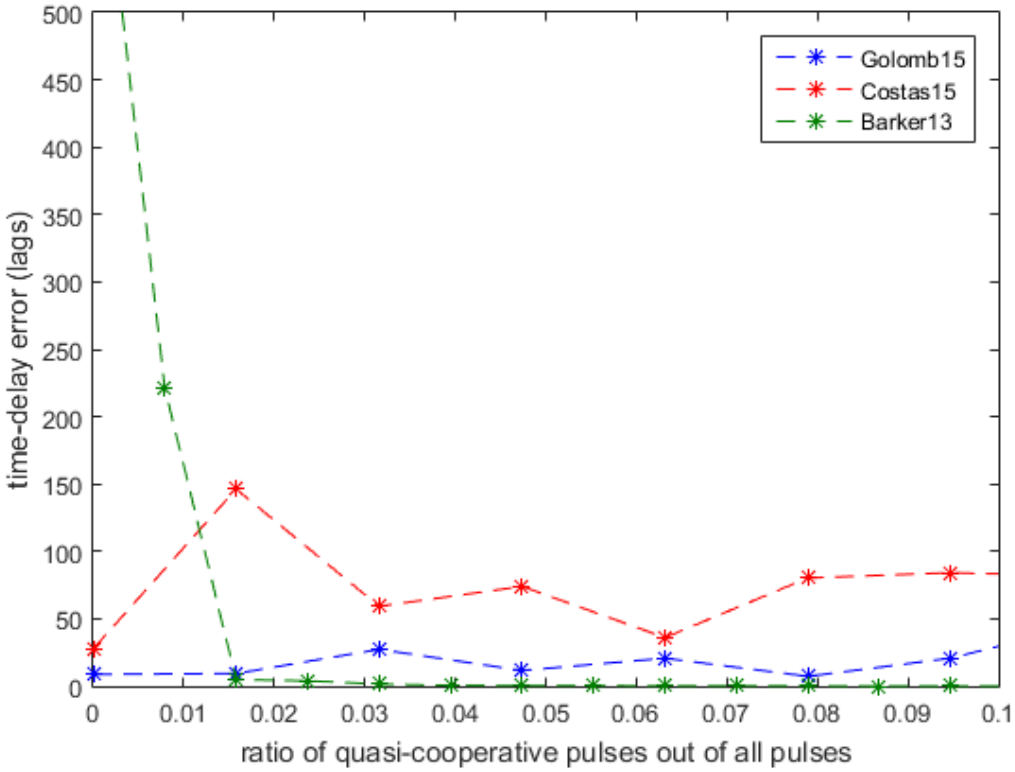


FIGURE 4.16: A comparison of time-delay estimation error between different waveform coding as a function of the ratio of quasi-cooperative coding.

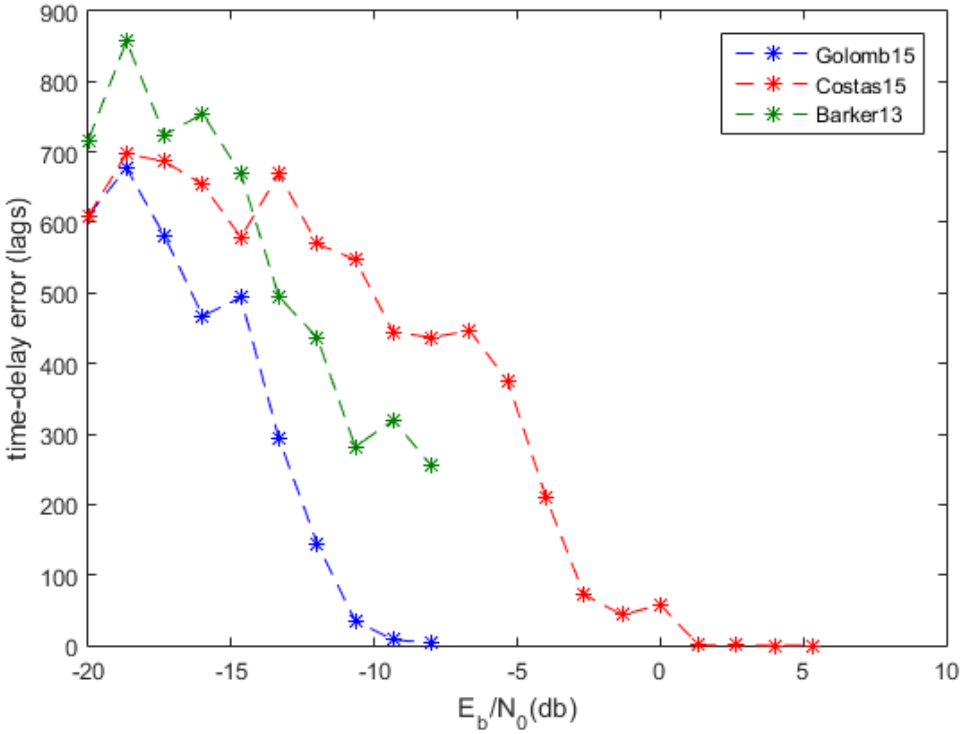


FIGURE 4.17: A comparison of time-delay estimation error between different waveform coding as a function of SNR.

5

Conclusions and Future Work

5.1 Conclusions

This work focused on two main challenges of backscatter communication: The strong self-interference and spread Doppler clutter that mask the information-bearing signal scattered from the transponder, and the measurement of the location of the backscatter device that is negatively affected by both the clutter and the modulation of the signal return.

This work proposed a channel coding framework for the backscatter channel leveraging a quasi-cooperative transponder and run-length limited coding to mitigate the background self-interference and spread-Doppler clutter with only a small decrease in the communication rate. The proposed method was generalized to both binary phase-shift keying and quadrature-amplitude modulation and provides an increase in rate by up to a factor of two compared with previous methods.

Additionally, this work analyzed the use of frequency modulation and bi-phase waveform coding for the radar waveform for high precision range estimation of the transponder location. Compared to previous methods, optimal range sidelobes are

achieved.

A phase discriminating algorithm is proposed to make it possible to separate the waveform coding from the communication coding, upon reception, and achieve localization with increased signal energy by up to 3 dB compared with previous reported results.

The joint communication-localization framework also enables a low-complexity receiver design because the same radio is used both for localization and communication.

Simulations comparing the performance of different codes corroborate the theoretical results and offer a possible trade-off between information rate and clutter mitigation as well as a trade-off between choice of waveform-channel coding pairs. Experimental results from a brass-board microwave system in an indoor environment are presented and discussed.

5.2 Future work - Optimal codes for backscatter communication channel

The RLL codes analyzed in this work were chosen to mitigate clutter and were chosen based on their specific spectrum shape and their DC nulling. However, clutter spectral distribution is unique for specific use cases of clutter and the RLL spectrum shaping did not optimally overlap with the clutter spectral distribution. An optimal way would be to design codes that fit a very specific clutter distribution (e.g. deep ocean surface). Such codes design framework exists (see Calderbank and Mazo (1991)) and would require to adapt it to the Doppler domain with careful consideration of the restricted alphabet of the tags.

5.3 Future work - Multi-phase waveform codes for backscatter communication

It is suggested to extend the current framework that allows all bi-phase waveform codes, to include multi-phase codes as well. The effect of multi-phase modulation on the receiver and the ability of the receiver to discriminate waveform code from the tag modulation needs to be analyzed.

Bibliography

Alevizos, P. N., Fasarakis-Hilliard, N., Tountas, K., Agadakos, N., Kargas, N., and Bletsas, A. (2014), "Channel coding for increased range bistatic backscatter radio: Experimental results," in *RFID Technology and Applications Conference (RFID-TA), 2014 IEEE*, pp. 38–43, IEEE.

Angerer, C., Langwieser, R., and Rupp, M. (2010), "RFID reader receivers for physical layer collision recovery," *Communications, IEEE Transactions on*, 58, 3526–3537.

Arthaber, H., Faseth, T., and Galler, F. (2015), "Spread-Spectrum Based Ranging of Passive UHF EPC RFID Tags," *Communications Letters, IEEE*, 19, 1734–1737.

Banerjee, S. R., Jesme, R., and Sainati, R. A. (2008), "Investigation of spatial and frequency diversity for long range UHF RFID," in *Antennas and Propagation Society International Symposium, 2008. AP-S 2008. IEEE*, pp. 1–4, IEEE.

Bharadia, D., Joshi, K. R., Kotaru, M., and Katti, S. (2015), "BackFi: High Throughput WiFi Backscatter," in *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, pp. 283–296, ACM.

Bi, Q., Zysman, G., and Menkes, H. (2001), "Wireless mobile communications at the start of the 21st century," *Communications Magazine, IEEE*, 39, 110–116.

Blasch, E. P. (2004), "Fusion of distributions for radar clutter modeling," in *Proc. of Int. Conf. on Information Fusion, June 28-July 1*.

Boyer, C. and Roy, S. (2013), "Space time coding for backscatter RFID," *Wireless Communications, IEEE Transactions on*, 12, 2272–2280.

Burns, R. W. (2004), *Communications: an international history of the formative years*, vol. 32, IET.

Calderbank, A. and Mazo, J. (1991), "Spectral nulls and coding with large alphabets," *Communications Magazine, IEEE*, 29, 58–67.

Carlowitz, C., Vossiek, M., Strobel, A., and Ellinger, F. (2013), "Precise ranging and simultaneous high speed data transfer using mm-wave regenerative active

backscatter tags," in *RFID (RFID), 2013 IEEE International Conference on*, pp. 253–260, IEEE.

Chawla, V. and Ha, D. S. (2007), "An overview of passive RFID," *Communications Magazine, IEEE*, 45, 11–17.

Cnaan-On, I., Thomas, S. J., Reynolds, M. S., and Krolik, J. L. (2014), "Multichannel radar backscatter communication and localization," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, pp. 76–80, IEEE.

Cnaan-On, I., Thomas, S. J., Krolik, J. L., and Reynolds, M. S. (2015), "Multichannel Backscatter Communication and Ranging for Distributed Sensing With an FMCW Radar," *Microwave Theory and Techniques, IEEE Transactions on*, 63, 2375–2383.

Cohen, S. A. (1972), "Cross-Ambiguity Function for a Linear FM Pulse Compression Radar," *Electromagnetic Compatibility, IEEE Transactions on*, pp. 85–91.

Curty, J.-P., Declercq, M., Dehollain, C., and Joehl, N. (2007), *Design and Optimization of passive UHF RFID Systems*, Springer.

D'Andrea, A. N., Mengali, U., and Reggiannini, R. (1994), "The modified Cramer-Rao bound and its application to synchronization problems," *Communications, IEEE Transactions on*, 42, 1391–1399.

Dardari, D., D'Errico, R., Roblin, C., Sibille, A., and Win, M. Z. (2010), "Ultrawide bandwidth RFID: The next generation?" *Proceedings of the IEEE*, 98, 1570–1582.

Durgin, G. D. and Rohatgi, A. (2008), "Multi-antenna RF tag measurement system using back-scattered spread spectrum," in *RFID, 2008 IEEE International Conference on*, pp. 1–8, IEEE.

Fawky, A., Mohammed, M., El-Hadidy, M., and Kaiser, T. (2014), "UWB chipless RFID system performance based on real world 3D-deterministic channel model and ZF equalization," in *Antennas and Propagation (EuCAP), 2014 8th European Conference on*, pp. 1765–1768, IEEE.

Franks, L. (1980), "Carrier and bit synchronization in data communication – A tutorial review," 28, 1107–1121.

Friis, H. T. (1946), "A note on a simple transmission formula," *proc. IRE*, 34, 254–256.

Garfinkel, S. and Rosenberg, B. (2006), *RFID: Applications, security, and privacy*, Pearson Education India.

Green, R. B. (1963), "The General Theory of Antenna Scattering," Ph.D. dissertation, Antenna Lab, The Ohio State University, United States – Ohio.

Greg, G. (2015), "The British Invention Of Radar," .

Griffin, J. D. and Durgin, G. D. (2008), "Gains for RF tags using multiple antennas," *Antennas and Propagation, IEEE Transactions on*, 56, 563–570.

Griffin, J. D. and Durgin, G. D. (2009a), "Complete link budgets for backscatter-radio and RFID systems," *Antennas and Propagation Magazine, IEEE*, 51, 11–25.

Griffin, J. D. and Durgin, G. D. (2009b), "Multipath fading measurements for multi-antenna backscatter RFID at 5.8 GHz," in *RFID, 2009 IEEE International Conference on*, pp. 322–329, IEEE.

Griffiths, D. J. and College, R. (1999), *Introduction to electrodynamics*, vol. 3, Prentice Hall Upper Saddle River, NJ.

Hansen, R. (1989), "RELATIONSHIPS BETWEEN ANTENNAS AS SCATTERERS AND AS RADIATORS," 77, 659–662.

Ingram, M. A., Demirkol, M. F., and Kim, D. (2001), "Transmit diversity and spatial multiplexing for RF links using modulated backscatter," *Signal*, 10, 3.

Johnson, C. R. and Sethares, W. A. (2004), *Telecommunication breakdown: concepts of communication transmitted via software-defined radio*, vol. 1, Prentice Hall.

Karam, G., Jeanclaude, I., and Sari, H. (1995), "A reduced-complexity frequency detector derived from the maximum-likelihood principle," *Communications, IEEE Transactions on*, 43, 2641–2650.

Kay, S. (1993), *Fundamentals of Statistical Signal Processing: Estimation Theory*, Fundamentals of Statistical Signal Processing, PTR Prentice-Hall.

La Porta, T. F., Maselli, G., and Petrioli, C. (2011), "Anticollision protocols for single-reader RFID systems: temporal analysis and optimization," *Mobile Computing, IEEE Transactions on*, 10, 267–279.

Lasser, G. and Mecklenbrauker, C. F. (2015), "Self-interference noise limitations of RFID readers," in *RFID (RFID), 2015 IEEE International Conference on*, pp. 145–150, IEEE.

Lathi, B. (1998), *Modern Digital and Analog Communication Systems*, Oxford series in electrical and computer engineering, Oxford University Press.

Lee, J., Choi, J., Lee, K. H., Kim, B., Jeong, M., Cho, Y., Yoo, H., Yang, K., Kim, S., Moon, S.-M., et al. (2007), "A UHF mobile RFID reader IC with self-leakage canceller," in *Radio Frequency Integrated Circuits (RFIC) Symposium, 2007 IEEE*, pp. 273–276, IEEE.

Lee, S.-R., Joo, S.-D., and Lee, C.-W. (2005), "An enhanced dynamic framed slotted ALOHA algorithm for RFID tag identification," in *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on*, pp. 166–172, IEEE.

Levanon, N. and Mozeson, E. (2004), *Radar signals*, John Wiley & Sons.

Liu, V., Parks, A., Talla, V., Gollakota, S., Wetherall, D., and Smith, J. R. (2013), "Ambient backscatter: wireless communication out of thin air," in *ACM SIGCOMM Computer Communication Review*, vol. 43, pp. 39–50, ACM.

Lunglmayr, M. and Huemer, M. (2010), "Least Squares Equalization for RFID," in *Near Field Communication (NFC), 2010 Second International Workshop on*, pp. 90–94, IEEE.

EPC Global US (2005), "Class 1 Generation 2 UHF RFID Protocol for operation at 860MHz-960MHz, version 1.0.9," Available online, *http://www.epcglobalus.org/*.

Miesen, R., Kirsch, F., and Vossiek, M. (2013), "UHF RFID localization based on synthetic apertures," *Automation Science and Engineering, IEEE Transactions on*, 10, 807–815.

Mohsenian-Rad, A.-H., Shah-Mansouri, V., Wong, V. W., and Schober, R. (2009), "Randomized multi-channel interrogation algorithm for large-scale RFID systems," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pp. 1–6, IEEE.

Nikitin, P., Rao, K., and Martinez, R. (2007), "Differential RCS of RFID tag," *Electronics Letters*, 43, 431 – 432.

Polastre, J., Szewczyk, R., and Culler, D. (2005), "Telos: enabling ultra-low power wireless research," in *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on*, pp. 364–369, IEEE.

Priya, S. and Inman, D. J. (2009), *Energy harvesting technologies*, vol. 21, Springer.

Proakis, J. (2000), *Digital Communications*, McGraw-Hill Science/Engineering/Math, 4 edn.

Proakis, J. G., Salehi, M., Zhou, N., and Li, X. (1994), *Communication systems engineering*, vol. 1, Prentice-hall Englewood Cliffs.

Ramakrishnan, D. and Krolik, J. (2009), "Adaptive radar detection in doubly nonstationary autoregressive Doppler spread clutter," *Aerospace and Electronic Systems, IEEE Transactions on*, 45, 484–501.

Richards, M. A. (2005), *Fundamentals of radar signal processing*, Tata McGraw-Hill Education.

Rife, D. and Boorstyn, R. R. (1974), "Single tone parameter estimation from discrete-time observations," *Information Theory, IEEE Transactions on*, 20, 591–598.

Safarian, A., Shameli, A., Rofougaran, A., Rofougaran, M., and De Flaviis, F. (2007), "An integrated RFID reader," in *2007 IEEE International Solid-State Circuits Conference. Digest of Technical Papers*.

Schouhamer-Immink, K. (1991), *Coding techniques for digital recorders*, Prentice Hall Professional Technical Reference.

Sekine, M., Ohtani, S., Musha, T., Irabu, T., Kiuchi, E., Hagisawa, T., and Tomita, Y. (1981), "Weibull-distributed ground clutter," *IEEE Transactions on Aerospace Electronic Systems*, 17, 596–598.

Skolnik, M. (2002), *Introduction to Radar Systems*, McGraw-Hill Science/Engineering/Math, 3 edn.

Springer, A., Gugler, W., Huemer, M., Reindl, L., Ruppel, C., and Weigel, R. (2000), "Spread spectrum communications using chirp signals," in *EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA*, pp. 166–170, IEEE.

Stern, H. P. and Mahmoud, S. (2003), *Communication Systems: Analysis and Design*, Prentice-Hall, Inc.

Stinco, P., Greco, M., Gini, F., and Rangaswamy, M. (2012), "Ambiguity function and Cramér–Rao bounds for universal mobile telecommunications system-based passive coherent location systems," *IET Radar, Sonar & Navigation*, 6, 668–678.

Stockman, H. (1948), "Communication by Means of Reflected Power," *Proc. of the IRE*, 36, 1196–1204.

Su, W., Alchazidis, N., and Ha, T. T. (2010), "Multiple RFID tags access algorithm," *Mobile Computing, IEEE Transactions on*, 9, 174–187.

Tandon, A., Motani, M., and Varshney, L. R. (2014), "On code design for simultaneous energy and information transfer," in *Information Theory and Applications Workshop (ITA), 2014*, pp. 1–6, IEEE.

Thomas, S. J., Wheeler, E., Teizer, J., and Reynolds, M. S. (2012), "Quadrature amplitude modulated backscatter in passive and semipassive UHF RFID systems," 60, 1175–1182.

Trees, H. L. V. (1992), *Detection, Estimation, and Modulation Theory: Radar-Sonar Signal Processing and Gaussian Signals in Noise*, Krieger Publishing Co., Inc.

Wang, J. and Katabi, D. (2013), "Dude, where's my card?: RFID positioning that works with multipath and non-line of sight," in *ACM SIGCOMM Computer Communication Review*, vol. 43, pp. 51–62, ACM.

Wang, J., Hassanieh, H., Katabi, D., and Indyk, P. (2012), "Efficient and reliable low-power backscatter networks," *ACM SIGCOMM Computer Communication Review*, 42, 61–72.

Ward, K. D., Watts, S., and Tough, R. J. (2006), *Sea clutter: scattering, the K distribution and radar performance*, vol. 20, IET.

Winkler, M., Faseth, T., Arthaber, H., and Magerl, G. (2010), "An UHF RFID tag emulator for precise emulation of the physical layer," in *Microwave Conference (EuMC), 2010 European*, pp. 1750–1753, IEEE.

Yen, C.-C., Gutierrez, A. E., Veeramani, D., and van der Weide, D. (2007), "Radar cross-section analysis of backscattering RFID tags," *Antennas and Wireless Propagation Letters, IEEE*, 6, 279–281.

Zhou, C. and Griffin, J. D. (2012), "Accurate phase-based ranging measurements for backscatter RFID tags," *Antennas and Wireless Propagation Letters, IEEE*, 11, 152–155.

Biography

Itay Menachem Cnaan-On was born in Beer-Sheva, Israel on November 12, 1980. He graduated from Harishonim High School in 1998.

Between 1999 and 2005 he served in the Israel Defense Force as a team leader in an elite technological unit. He graduated from the officer academy and his last rank was Lieutenant.

He attended Tel-Aviv University from 2006 to 2010, and graduated with a Bachelor of Science degree in Electrical and computer engineering.

Between 2009 and 2011 he served as a software development team leader in Essence group, an Internet of Things wireless sensors developer company.

Itay entered graduate school at Duke University in 2011. He joined Dr. Jeff Krolik's lab for Sensor array and multipath. During that time, he served as a reseach assitant and teaching assistant for multiple courses.

He was awarded the National Science Foundation IGERT fellowship for Wireless Intelligent Sensor Networks (WISeNet) from 2012 to 2014.

In 2014 he was a visitng researcher at the Institute of Microwave and Photonics at the University of Erlangen-Nuernberg.

Itay earned a Master of Science degree in Electrical and Computer engineering from Duke university in 2014.