TECHNICAL UNIVERSITY OF CRETE
ELECTRICAL AND COMPUTER ENGINEERING DEPARTMENT
TELECOMMUNICATIONS DIVISION

Backscatter Radios with LimeSDR

by

Giannakopoulos Konstantinos Orestis

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DIPLOMA OF

ELECTRICAL AND COMPUTER ENGINEERING

July 2020

THESIS COMMITTEE

Professor Aggelos Bletsas, *Thesis Supervisor*
Professor George N. Karystinos
Associate Professor Antonios Deligiannakis

Abstract

This dissertation presents two backscatter radio applications for wireless sensor networks with the low-cost software-defined radio (SDR) LimeSDR platform. Two different architectures are developed. The first application implements a monostatic receiver, where the LimeSDR is configured as both the RF-tag's illuminator, as well as the receiver of the backscattered signal. It is found that the monostatic architecture in combination with the transmitting power capabilities of the LimeSDR board (2 dBm output power) can achieve a range of 9.4 meters. The range coverage increased to 13.7 meters with the use of an external amplifier. The second application presents a reader for ambiently-powered scatter radio sensors that exploit the FM broadcast signals for illumination. In this architecture, the source of the illuminating signal is located 7 kilometers away. The backscattered signal is also an FM audio signal with a frequency that corresponds to the sensors' measurement. The receiver demodulates the signal and detects the frequency using periodogram-based Fourier analysis. The maximum range achieved between the sensor and the reader for this architecture, with a root mean square error (RMSE) less than 200 Hz, was 7 meters. Both applications implement low-cost radio link communication exploiting the fact that scatter radio, in principle, requires low energy consumption and simple hardware demands. Additionally, a WiFi adhoc network link was implemented with a USB adapter to transfer the sensed information to a central node/base station. TCP and UDP protocols were tested for range maximization between the reader and base station. UDP protocol achieved the maximum range coverage of approximately 146 meters. Experiments on soil moisture measurements were conducted to test the efficiency and the range coverage of each system.

Thesis Supervisor:Professor Aggelos Bletsas

Acknowledgements

As my undergraduate studies are coming to an end, I would like to to thank all the people who supported me during my academic life. Foremost, I would like to express my sincere gratitude to my supervisor professor Mr. Aggelos Bletsas for all the guidance and the knowledge provided during my dissertation. I am more than grateful to my family, who invested in my education all these years and encouraged me through this period. None of that could be possible without their support. Last but not least, I would like to thank all my friends who made all these years special.

Table of Contents

List of Figures

Chapter 1

Introduction

1.1   Motivation

The environmental crisis of the modern era, has increased the need for protection and management optimization of natural resources. Water-saving is the main issue of interest, especially in agricultural production. Therefore, a need for cultivation monitoring has been raised, in order to adjust the agricultural procedures according to the plants' microclimate condition. Apart form water-saving, chemical usage containment, soil pH controlling are some other main areas of interest for monitoring purposes. Further more, precision agriculture concept contributes to higher quality products, expenditure minimization, and eco-friendly procedures.

Wireless sensor network (WSN) technology is used for large scale field monitoring, with a dense layer of sensors providing measurements for a variety of metrics. Conventional wireless sensor networks use expensive, energy-consuming protocols (e.g. Bluetooth), which sometimes leads to non-profitable applications, regarding large scale network deployments. As a consequence, the cost of each node of the network should be minimized.

Scatter radio principles can provide low-cost and low-energy consumption solutions for the implementation of such networks, considering the fact that the nodes do not transmit their information actively. Instead, they modulate their data on the reflection of an illuminating signal. The energy consumption for the data transmission of each node is equal to the cost of a toggling switch, as there is no use of active RF-components like phase locked loops, amplifiers, filters, etc.

Software defined radios (SDRs) are appropriate for the implementation of these networks' RF front-end, due to their flexibility for customized experi-

ments and prototyping. There is a large community working on open source projects, therefore there is a rapid development on this technology. LimeSDR is a low-cost software defined radio board with great capabilities and it is chosen for the implementation among other commercially available SDRs after evaluating both its capabilities and the current work's requirements.

1.2   Objective

The objective of this dissertation is the implementation of low cost scatter radio applications for environmental monitoring, with a commercially available software-defined radio, LimeSDR, as the RF-frontend receiver. The main benefit of LimeSDR is the significantly lower price compared to other commercially available software define radios, which drops further the total cost of the application. The performance of the board in scatter radio applications is evaluated by experiments. The hardware, features, and specifications of the board will be analytically presented in the next chapter.

1.3   Current State of Art

The novelty this work offers, is the evaluation of LimeSDR as a compact reader for wireless sensor applications based on backscatter radio link communication. Currently, Universal Software Radio Peripheral (USRP) devices, produced by Ettus Research, have been used for the development of wireless sensor network applications in the context of past research with a variety of architectures [4], [5], [6].The range coverage has been increased from tens to hundreds of meters with the use of variant topologies, namely; bistatic, multistatic, etc as the outcome of this work. Generally, there is a rapid growth of interest in scattering radio technology over the past few years besides WSN, with radio frequency identification (RFID) being the most common commercial use of backscatter technology.

1.4 Outline

- **Chapter 1** introduces the concept covered in this thesis.

- **Chapter 2** defines the communication system of software defined radios and highlights its benefits. Moreover, it presents the LimeSDR board components, features and specifications. Finally, the key principle of the scatter radio is explained.

- **Chapter 3** covers the implementation of the monostatic reader. Basic theory, experimental setup and board configuration are shown.

- **Chapter 4** covers the implementation of a reader in ambient architecture. Basic theory, experimental setup, and board configuration are analyzed.

- **Chapter 5** reviews the experimental results, and evaluates the achieved performance.

- **Chapter 6** summarizes the topics of this work and also suggests potential future work.

Chapter 2

Background

This chapter covers some background knowledge for the better understanding of the dissertation. The communication system of software defined-radios is explained and it is compared with conventional radio devices. Additionally, the LimeSDR board is presented along with the software setup required for the implementation of this thesis. Finally, the scatter radio principle is described.

2.1   Software Defined Radio (SDR)

Software-defined radio (SDR), as depicted in Fig. 2.1, is a radio communication system, where all the hardware components (e.g filters, mixers, modulators etc), are implemented through software, on a personal computer or an embedded system. Conventional radios are constrained into dedicated use, due to their specified hardware components, with frequency range being limited and defined by protocols. On the contrary, software-defined radio devices have reconfigurable components and wide tuning frequency range, which provides great flexibility for prototyping development. Furthermore, the power of digital processing provides great advantages over the traditional radios. Significant progress has been made over the past few years in this field, as the performance has risen and the hardware cost has been reduced [7].
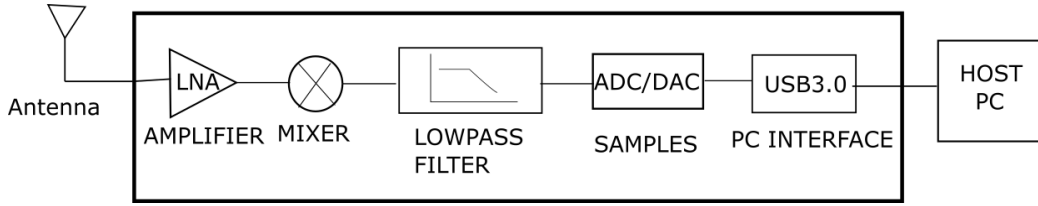
Figure 2.1: Typical SDR architecture.

2.2 LimeSDR

LimeSDR board, illustrated in Fig. 2.2, is a low-cost software-defined radio platform [8], supporting a variety of wireless communication standards, namely; LTE, GSM, LoRa, Bluetooth, Zigbee, RFID, etc. The offered features give primates advantages over other commercially available SDRs. It is the first SDR with integrated snappy Ubuntu core, which means applications can be developed and downloaded from every developer around the world (open source software and hardware). Additionally, LimeSDR has a powerful full-duplex transceiver (2x2 MIMO), with great performance at metrics like frequency range, bandwidth etc, that will be presented analytically. Integrated filtering for both channels reduces the needs of external filters. The key advantage of this software defined radio, is the low price in the order of few hundreds of US dollars, which makes it a very cost effective solution compared to other software define radios platforms with similar capabilities.

2.2.1 Features and Specifications

Features and specification of the board as presented in [8]. The components of the board are shown in Fig. 2.3.

- RF Transceiver: Lime Microsystems LMS7002M MIMO FPRF.

- FPGA: Altera Cyclone IV EP4CE40F23,

- Memory: 256 MBytes DDR2 SDRAM.

- USB 3.0 controller: Cypress USB 3.0 CYUSB3014-BZXC.

- Oscillator: Rakon RPT7050A @30.72MHz.

- Continuous frequency range: 100 kHz to 3.8 GHz.

- Bandwidth: 61.44 MHz.

- RF connection: 10 U.FL connectors (6 Rx, 4 Tx).

- Power Output (CW): up to 10 dBm (depending on frequency).

- Multiplexing: 2x2 MIMO.

- Power: micro USB connector or optional external power supply.

- Status indicators: programmable LEDs.
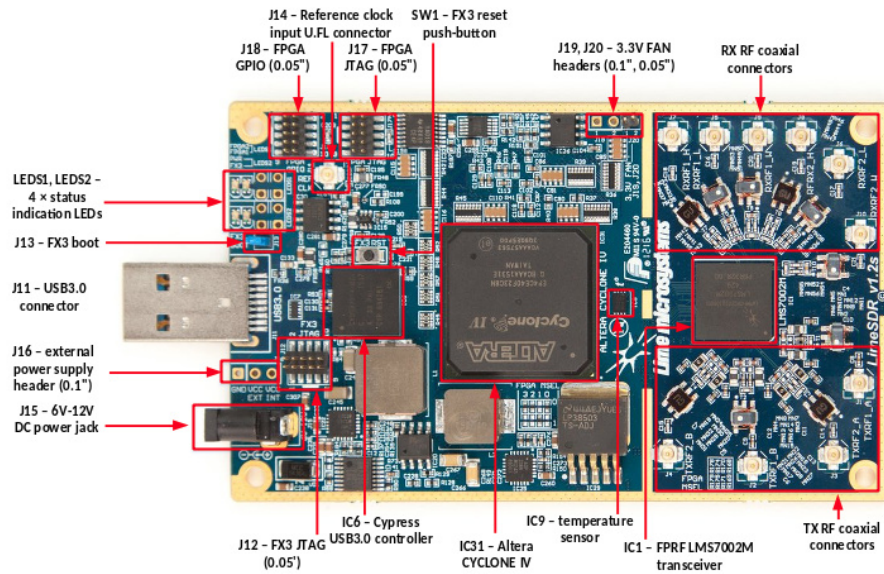
- Dimensions: 100 mm x 60 mm.

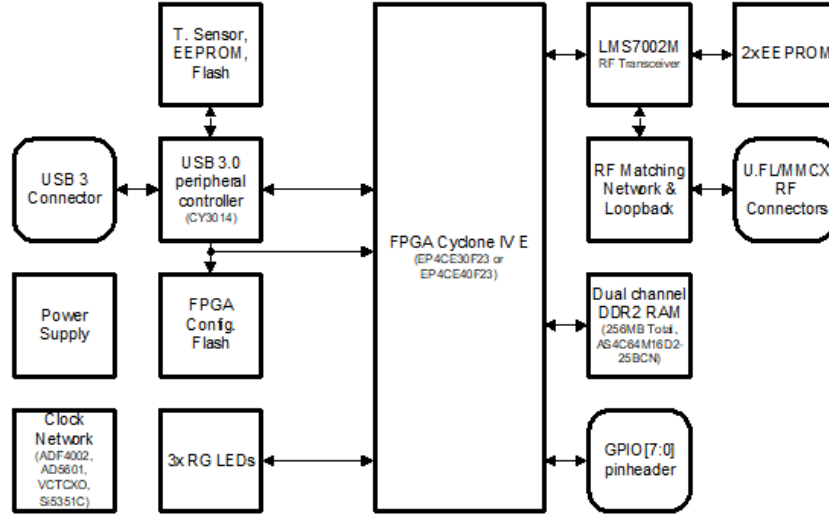Figure 2.2: LimeSDR-USB board overview by MyRiadRF [1].

Figure 2.3: Development Board Block Diagram by MyriadRF [2].

LMS7002M [9]: The transceiver chip, in Fig. 2.4, determines the RF functionality and performance of the board. A full duplex transceiver is consisted of two transmitter/receiver pairs. Each channel has three receive and two transmit connectors. On the receive side, each connector corresponds to an analog path with a dedicated LNA (RXLNA), optimised for narrow or wide band operations. Each path has three stages of amplifiers in total: low noise amplifier (LNA), trans-impedance amplifier (TIA) and programmable gain amplifier (RXPGA). Furthermore, the receive chain also consists of low pass filters (RXLPF), mixers for baseband conversion of the RF signal and an ADC converter. On the transmit side, each path includes DAC, a low pass filter (TXLPF), mixer and power amplifier driver (TXPAD). The ADCs and DACs of LimeSDR have 12 bits for quantization, with a dynamic range of approximately $DR = 72$ dB. Both Tx and Rx mixers are driven from two separate synthesizers, with same reference clock source in case of full duplex operation, or a single PLL (TXPLL) can drive both mixers in case of half-duplex applications. This feature reduces the frequency or phase mismatch between the transmitter and the receiver.
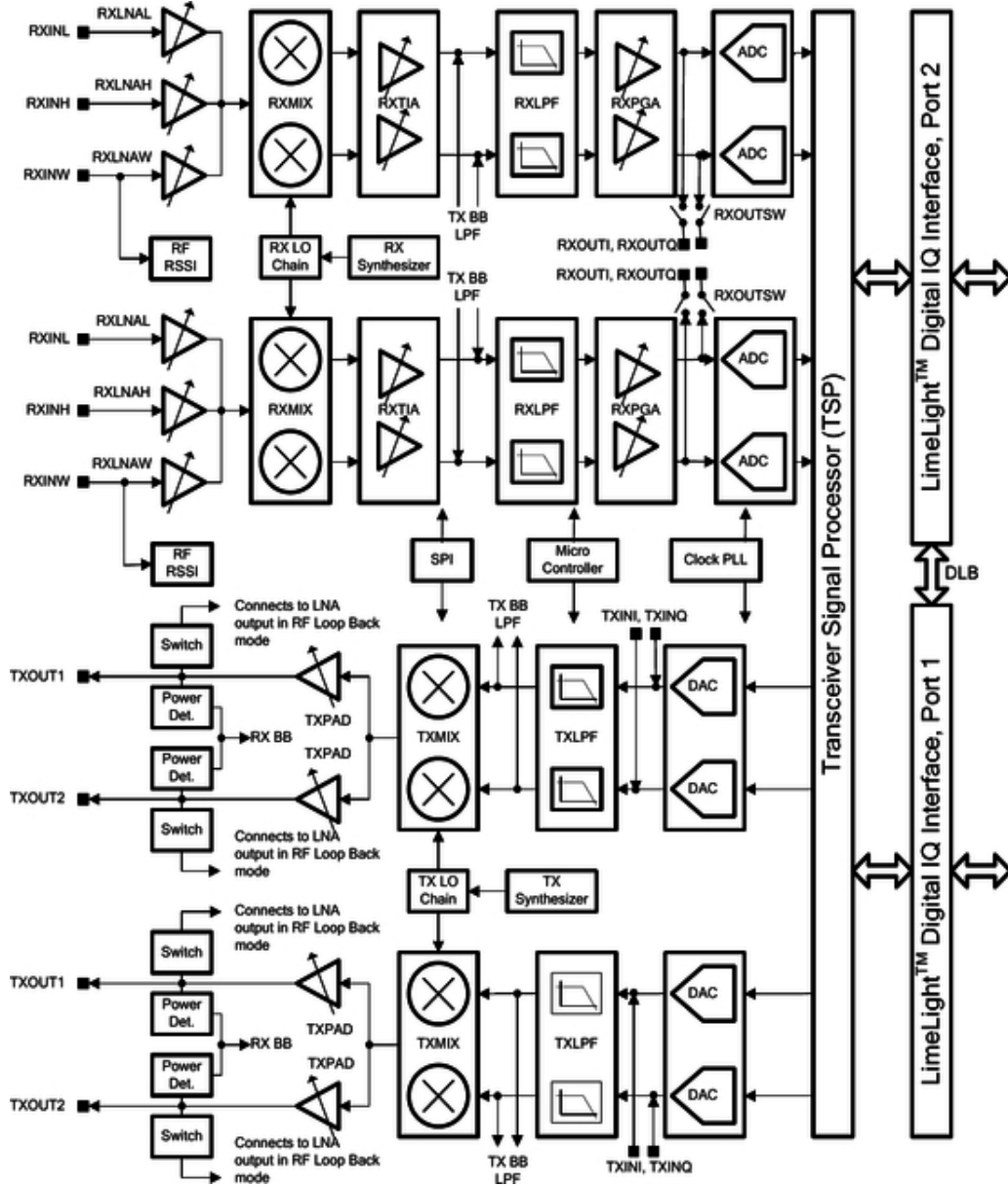
Figure 2.4: Transceiver functional block diagram by MyriadRF [3].

2.3   Software Setup

For radio application implementation besides hardware, software toolkits are necessary to carry out the signal processing and logic to the host computer. **GNU Radio** [10] is a free and open-source development toolkit, providing

signal processing blocks such as filters, Fourier analysis, etc for the development of software define radio applications. The connection of the processing blocks produces a final block diagram or as it is called, flowgraph. Additionally, GNU Radio has great flexibility as it enables the creation of custom blocks, if specific processing is required.

GNU Radio is a high-level platform, therefore, some extra layers are necessary to control the low-level LimeSDR hardware from GNU radio and complete the software setup.

1. **Lime suite [11]**: Lime Suite is a collection of software supporting the hardware of LimeSDR, drivers for the transceiver chip (LMS7002M) that allows the configuration and callibration of the transceiver.

2. **SoapyLMS7 [12]**: SoapyLMS7 allows LimeSuite devices to interface with applications that use the SoapySDR API such as GNU Radio.

3. **gr-limesdr [13]**: Plugin for GNU Radio user interface.

2.4 Scatter Radio

The scatter radio principle is based on the idea that instead of using active components to transmit the desirable information, a node may reflect induced RF signals to modulate the data [5]. A signal called carrier, which is usually a constant wave (CW) is used to illuminate the RF-tag. The antenna of the tag has an impedance Z_{source} and it is terminated to different loads through an impedance switch. If the termination load is not matched with the antenna load, i.e $Z_{source} \neq Z_{load}^*$, a portion of the power destined for the load will be reflected back to the source. The transition between the different loads causes changes to the amplitude and/or the phase of the induced signal. Therefore, the signal is modulated and reflected back from the same antenna. As a next step, a receiver captures, demodulates, decodes the scattered signal, and obtains the information of the RF-tag.

Scatter radio technology has been mainly used at commercial radio frequency identification (RFID) systems that identify products or people. This

technology could be of great use in large wireless sensor networks application deployment. The energy consumption and hardware demands of the RF-tags are extremely low. The data modulation is achieved only by load switching and there is no use of mixers or any active RF-component. In addition, the cost per node is minimized. The key disadvantage of this technology is the limited range coverage. However, due to research presented during the last years, usage of different modulations, more advanced hardware and different architectures, have achieved a significant range extension. For the purpose of this work, the reader is implemented by two different architectures based on the LimeSDR board.

Chapter 3

Monostatic SDR Reader

3.1 Basic Theory

3.1.1 Monostatic Architecture

In monostatic architecture, as it is shown in Fig. 3.1, the software-defined radio incorporates both the carrier emitter, which illuminates the RF-tag and the reader that captures and decodes the signal. This architecture can be implemented with the capabilities that LimeSDR provides. The transmit chain of the board transmits a constant wave (carrier emitter) and the receive chain refers the reader. The main disadvantage of monostatic architecture is the round-trip path loss where SNR drops significantly with the fourth power of the tag to reader distance, which sets a limit to range coverage. The benefit of monostatic architecture is that it makes the signal model simpler, due to the fact that both transmit and receive chain share the same local oscillator. Therefore, there is neither carrier frequency offset nor phase mismatch between the transmitter and the receiver.
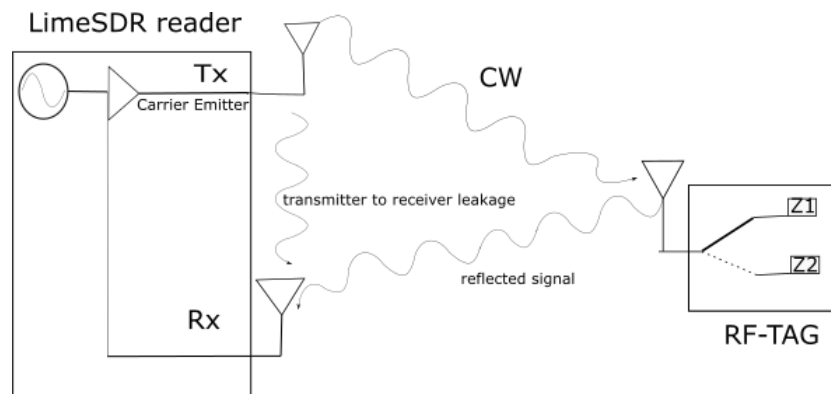

Figure 3.1: Monostatic architecture.

3.1.2 Signal Model

Carrier emitter transmits a continuous sinusoidal wave (CW) at carrier frequency F_c whose complex baseband equivalent can be written as [4]:

$$c(t) = \sqrt{2P_c}e^{j(2\pi F_c t + \phi_c)}, \tag{3.1}$$

where P_c, F_c and ϕ_c are the power, frequency and phase of the carrier respectively. The CW propagates through the carrier-to-tag flat-fading channel h_{CT}, which is defined by the equation [6]:

$$h_{CT}(t) = \alpha_{CT}\delta(t - \tau_{CT}), \tag{3.2}$$

and the phase introduced by propagation delay is $\phi_{CT} = 2\pi\tau_{CT} \in [0, 2\pi)$. RF-tag, as described at chapter 2.4, switches the antenna between two load reflection coefficients Γ_0 and Γ_1 in order to modulate the data. The antenna load reflection coefficient is given by the following equation:

$$\Gamma_i = \frac{Z_i - Z_a^*}{Z_i + Z_a}, \tag{3.3}$$

where Z_i refers to the tag load with $i \in \{0, 1\}$ and Z_a to the antenna impedance. The switch toggles between the two loads with two distinct frequencies F_0 and F_1. The RF-tag's complex baseband signal can be written as:

$$x(t) \triangleq \alpha_x(t)e^{j\phi_x(t)} = A_s - \Gamma(t), \tag{3.4}$$

where A_s is a complex value that depends on the antenna characteristics like the geometry and the materials used for the construction, which is called structural mode. $\Gamma(t) \in \{\Gamma_0, \Gamma_1\}$ is the reflection coefficient changes as a function of time. The amplitude $\alpha_x(t)$ is:

$$\alpha_x(t) \triangleq |A_s - \Gamma(t)|, \tag{3.5}$$

and the phase $\phi_x(t)$ is :

$$\phi_x(t) \triangleq \angle[A_s - \Gamma(t)] \tag{3.6}$$

the angle of the complex quantity $A_s - \Gamma(t)$ in radians. When the constant wave $c(t)$ illuminates the tag, a scattered signal is produced and the waveform can be given from the equation:

$$x_m(t) = s\left(\left(A_s - \frac{\Gamma_0+\Gamma_1}{2}\right) + \frac{\Gamma_0-\Gamma_1}{2}u_i(t)\right) A_{CT}e^{-j\phi_{CT}}c(t)$$

$$= s\left(u_0 + \frac{\Gamma_0 - \Gamma_1}{2}u_i(t)\right) A_{CT}e^{-j\phi_{CT}}c(t), \tag{3.7}$$

where $u_i(t)$ is the modulation waveform of bit i $\in \{0,1\}$, depending on the modulation, u_0 is a dc term which depends from antenna structural mode A_s and the reflection coefficients Γ_0 and Γ_1. The term s depends from the tag's scattering efficiency and the antenna gain towards the specific direction.

The received signal at the reader is a superposition of the RF-tag reflected signal and leakage from the carrier emitter that passes through tag to reader channel $h_{TR}(t) = \alpha_{TR}\delta(t - \tau_{TR})$ and carrier to reader channel $h_{CR}(t) = \alpha_{CR}\delta(t - \tau_{CR})$ respectively. The phase induced from propagation delay is $\phi_{TR} = 2\pi\tau_{TR}$, $\phi_{CR} = 2\pi\tau_{CR}$ with ϕ_{TR}, $\phi_{CR} \in [0, 2\pi)$. Conclusively, the received signal at the SDR receiver can be presented as:

$$y(t) = \alpha_{CR}e^{-j\phi_{CR}}c(t) + \alpha_{TR}e^{-j\phi_{TR}}x_m(t) + n(t) \tag{3.8}$$

$$= A\left(\alpha_{CR}e^{-j\phi_{CR}} + \alpha_{CT}\alpha_{TR}e^{-j(\phi_{CT}+\phi_{TR})}s\left(u_0 + \frac{\Gamma_0-\Gamma_1}{2}u_i(t)\right)\right)e^{j(2\pi F_c t+\phi_c)}+n(t).$$

To simplify the notation we can set the following abbreviations :

- $\phi_0 = \phi_{CR} + \phi_c$

- $\phi_1 = \phi_{CT} + \phi_{CR} + \phi_c$

- $\phi_2 = \phi_1 + \angle|\Gamma_0 - \Gamma_1|$

- $m_0 = A_c\,\alpha_{CR}$

- $m_1 = \alpha_{CT}\,\alpha_{TR}\,s\,\frac{|\Gamma_0-\Gamma_1|}{2}$

- $m_2 = A_c \; \alpha_{CT} \; \alpha_{TR} \; s \; u_0$

therefore, the equation can be written as:

$$y(t) = \left(m_0 e^{-j\phi_0} + m_2 e^{-j\phi_1} + m_1 e^{-j\phi_2} u_i(t)\right) e^{j2\pi F_c t} + n(t) \qquad (3.9)$$

with i$\in \{0,1\}$ and n(t) is a complex Gaussian random process corresponding to the thermal noise at the receiver. As a next step, the receiver has to achieve bit-level synchronization based on energy or preamble correlation, and then the received signal is sampled with period T_s. The baseband sampled version of the received signal can be written as:

$$y(k) \triangleq y(kT_s) = \left(m_0 e^{-j\phi_0} + m_2 e^{-j\phi_1}\right) + m_1 e^{-j\phi_2} u_i(kT_s) + n(kTs), \quad (3.10)$$

where n(kT_s) is the k-th Gaussian noise sample:

$$n(kT_s) \sim \mathcal{CN}\left(0, \, 2\sigma_n^2\right).$$

The low-pass power spectral density (PSD) of the complex Gaussian process n(t) is given by:

$$S_{n,n}(F) = \begin{cases} \frac{N_0}{2}, & |F| \leq W \\ 0, & elsewhere, \end{cases} \qquad (3.11)$$

where W is the base-band receiver bandwidth and each noise sample has power:

$$\epsilon[|n[k]|^2] = 2\sigma_n^2 = N_0 W. \qquad (3.12)$$

After synchronization and sampling, the receiver has to detect the FSK symbols. In Frequency Shift Keying modulation, each information symbol produces a modulation waveform of frequency F_i. The frequencies must have specific spacing among them for orthogonality assurance $|F_i - F_j| = k\frac{1}{T}$, where T is the bit duration with $k \in \mathbb{N}$ and $i \neq j$. In scatter binary FSK there are two distinct frequencies F_i for switching between two reflection coefficients namely; Γ_0, Γ_1. One frequency for each transmitting symbol, which

corresponds to bit value. The waveform of frequency F_i can be written as:

$$u_i(t) = \frac{4}{\pi}\cos(2\pi F_i t + \Phi_i)\Pi_T(t), i \in \{0,1\}, \qquad (3.13)$$

where $\Pi_T(t)$ is the modulation pulse which in each specific case is a rectangular pulse of duration T:

$$\Pi_T(t) = \begin{cases} 1, & 0 \leq t \leq T \\ 0, & elsewhere. \end{cases} \qquad (3.14)$$

$\Phi_i \sim U[0, 2\pi)$ corresponds to the phase mismatch between the RF-tag and the receiver at the i-ith bit transmission assuming that Φ_0, Φ_1 are constant and independent during a coherence window. The digitized sampled signal with B-FSK modulation can be written as:

$$y(kT_s) = \left(m_0 e^{-j\phi_0} + m_2 e^{-j\phi_1}\right) + \frac{4}{\pi}m_1 e^{-j\phi_2}\cos(2\pi F_i kT_s + \Phi_i)\Pi_L(k) + n(k),$$
$$(3.15)$$

with i$\in \{0,1\}$, L is the oversampling factor L=$\frac{T}{T_s}$ of the receiver and $\Pi_L(k)$ is the oversampled version of the modulation pulse $\Pi_T(t)$. The DC terms in the parenthesis of the equation above do not contribute with any information. Therefore, they can be excluded by using a DC blocking filter. After filtering the waveform, the following equation is unfolded:

$$y(k) = \frac{2}{\pi}m_1 \left(e^{j(2\pi F_i kT_s + \Phi_i - \phi_2)} + e^{-j(2\pi F_i kT_s + \Phi_i + \phi_2)}\right)\Pi_L(k) + n(k). \qquad (3.16)$$

The difference between classic and scatter B-FSK is now clearly defined. In scatter B-FSK two subcarriers are created for each frequency F_i at $\pm F_i$ as we can see two complex basis functions of the equation 3.2. However, the classic B-FSK provides only one subcarrier for each F_i. Therefore, for a classic B-FSK receiver, there would be loss of information due to the fact that the subcarriers are not taken under consideration at the negative semi-axis.

For the bit detection, four correlators are utilized, one for each subcarrier frequency[14].

$$r_0^+ = \sum_{k=-\infty}^{\infty} y[k](\Pi_L(k)e^{+j2\pi F_0 kT_s})^* = \sum_{k=0}^{L-1} y[k]e^{-j2\pi F_0 kT_s} =$$

$$\frac{2}{\pi} m_1 \sum_{k=0}^{L-1} e^{+j[2\pi(F_0 - F_i)kT_s + \Phi_i - \phi_2]} + n_0^+, \tag{3.17}$$

where L are the samples that are processed by each correlator in order to extract the statistics and $n_0^+ = \sum_{k=0}^{L-1} n[k]e^{+j2\pi F_0 kT_s}$ is the sum of L independent complex Gaussians. Similarly, the rest of the formulas regarding the correlators are given by the equations:

$$r_0^- = \frac{2}{\pi} m_1 \sum_{k=0}^{L-1} e^{-j[2\pi(F_0 - F_i)kT_s + \Phi_i - \phi_2]} + n_0^-,$$

$$r_1^+ = \frac{2}{\pi} m_1 \sum_{k=0}^{L-1} e^{+j[2\pi(F_1 - F_i)kT_s + \Phi_i - \phi_2]} + n_1^+,$$

$$r_1^- = \frac{2}{\pi} m_1 \sum_{k=0}^{L-1} e^{-j[2\pi(F_1 - F_i)kT_s + \Phi_i - \phi_2]} + n_1^-,$$

where $n_0^-, n_0^+, n_1^-, n_1^- \sim \mathcal{CN}(0, 2\sigma_n^2)$ are statistically independent random variables , as they are projections of Gaussian random process $n(t)$ on the orthogonal basis$\in \{e^{-j2\pi F_0 t}\Pi_T(t), e^{+j2\pi F_0 t}\Pi_T(t), e^{-j2\pi F_1 t}\Pi_T(t), e^{+j2\pi F_1 t}\Pi_T(t)\}$
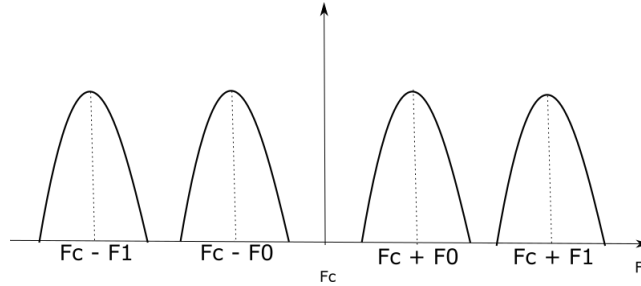

Figure 3.2: Passband spectrum for scatter B-FSK

In the first case, when bit "0" is transmitted, the outputs of the correlators will be:

$$r_0^+ = \frac{2m_1 L}{\pi} e^{-j\phi_2} e^{+j\Phi_0} + n_0^+,$$

$$r_0^- = \frac{2m_1 L}{\pi} e^{-j\phi_2} e^{+j\Phi_0} + n_0^-,$$

$$r_1^- = n_1^-,$$

$$r_1^+ = n_1^+,$$

and in the second case when bit "1" is transmitted, the outputs of the correlators will be:

$$r_0^- = n_0^-,$$

$$r_0^+ = n_0^+,$$

$$r_1^+ = \frac{2m_1 L}{\pi} e^{-j\phi_2} e^{+j\Phi_1} + n_1^+,$$

$$r_1^- = \frac{2m_1 L}{\pi} e^{-j\phi_2} e^{+j\Phi_1} + n_1^-,$$

After the extraction of statistics, a detector is utilized for the decision of the symbol:

$$z_1 \triangleq |r_1^-|^2 + |r_1^+|^2 \underset{}{\overset{H_1}{\gtrless}} |r_0^-|^2 + |r_0^+|^2 \triangleq z_0. \tag{3.18}$$

3.2   Experimental Setup

The experimental setup in this work consists of the RF-tag, the LimeSDR and the host PC that carries out the signal processing, as shown in Fig.3.3. LimeSDR is used for both the RF-tag's illumination and the reception of the reflected signal. Both transmit and receive chains are tuned in the UHF band in the frequency of 868 MHz, which is the European ISM band. LimeSDR configuration is handled via software as far as metrics are concerned, namely; frequency, sampling rate, oversampling factors, gains, and so on so forth, which will be presented later on. It is connected to the host PC with USB3.0 adapter for data transferring. The data is transferred to the host PC and signal processing is executed through GNU Radio software environment. Scat-

ter radio applications work at low bit-rate, as bandwidth capabilities of the LimeSDR's are more than sufficient for signal capturing. The RF-tags that are used for experiments consist of a MCU, a SMA antenna connector and a single RF-transistor. The implementation of the tags was held in the context of a previous research [14] and it is not the main topic of work presented on this chapter.
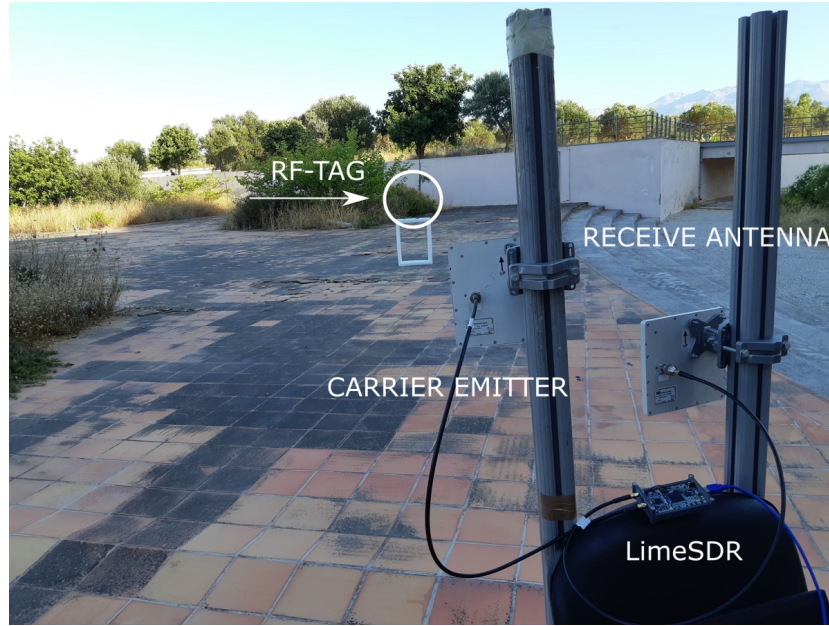

Figure 3.3: Experimental Setup.

3.2.1 Drone Setup

An alternative setup is configured on a drone. The host PC is replaced by an odroid and LimeSDR-mini is used instead of LimeSDR-USB, as it is illustrated in Fig.3.4. The mini version of the LimeSDR board is even more inexpensive, has a half duplex transceiver (1x1), which proves to be sufficient for the current application. The smaller size of that board is more convenient for the drone application. The monostatic architecture enables the drone to scan the field and take measurements while flying above the RF-tags. The difficulties mostly took place on practical side of the experiment. The drone

had to fly as stable as possible above the designated region of the tag, with its antennas pointing to the right direction.
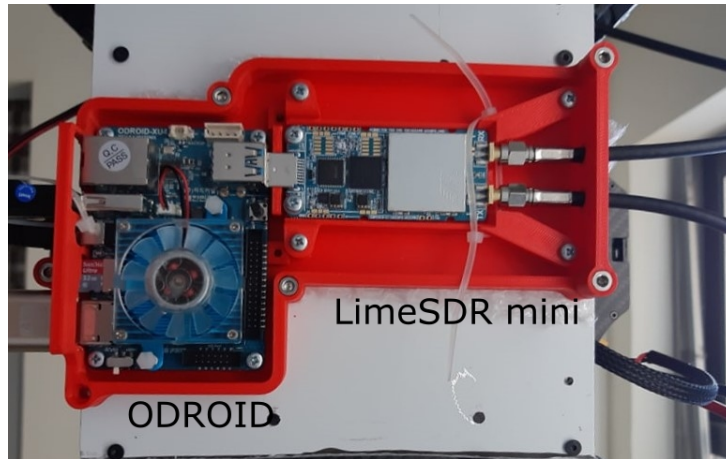

Figure 3.4: Drone setup: Bottom view of LimeSDR mini and odroid.

Figure 3.5:   Drone setup: Antennas.

3.3   LimeSDR Configuration

The board configuration is implemented according to the documentation [15].
Transmit chain: Transmit chain is responsible for the carrier emitter which illuminates the tag. The carrier is a constant wave at 868 MHz.

- Center frequency: 868 MHz.

- Sampling Rate: 1 MHz. Sampling rate of constant wave. This setting should match in transmitter and receiver for the same device.

- Oversampling factor: 32. Higher clock rates achieve better functionality of the LimeSDR board.

- Gain: Set to maximum value 60 dB. Transmission output power of LimeSDR is experimentally measured 2 dBm.

- NCO- numerically controlled oscillator is deactivated.

- Calibration bandwidth: 0 (deactivated). This setting should be equal to signal bandwidth. The signal is a constant wave.

- PA path: Select active power amplifier path of the channel, BAND1 is selected.

- Antenna selection: Select hardware port to be used for transmit.Value "1" is set that correspond to port Tx1-1.

- Digital filter bandwidth: Deactivated.

- Analog filter bandwidth: 5 MHz.

Receive chain: Receive chain is responsible for capturing the reflected signal and drive the data from LimeSDR to the host PC for the signal processing.

- Center frequency: 868 MHz.

- Sampling Rate: 1 MHz sufficient sampling rate for low bit-rate scatter radio applications.

- Oversampling factor: 32. Similarly as it is mentioned at the transmit chain above, the aim is to oversample the analog to digital converter (ADC) to improve SNR with high clocking rates.

- Gain: Set to maximum value 70 dB. As it is shown at Fig. 2.4, the RX gain is divided to three stages,the low noise amplifier (RXLNA) , the trans-impedance amplifier (RXTIA), the programmable gain amplifier (RXPGA). The drivers of the board decide about the gain distribution automatically.

- NCO- numerically controlled oscillator is deactivated.

- Calibration bandwidth: 0 (deactivated). There is no need for calibration in narrow band operations. This setting has to be equal to the signal's bandwidth with minimum value 2.5 MHz.

- Antenna selection: Each receive port has specified use depended on frequency. For the current narrow band application Value "1" is set that correspond to port $RX1_H$.

- LNA path: Select active low-noise amplifier path of the channel, LNAH is selected.

- Digital filter Bandwidth: Digital filter is deactivated.

- Analog filter bandwidth: 5 MHz.

Chapter 4

Ambient (Bistatic) SDR Reader

This chapter presents a reader for backscatter sensors, that exploits the signal of the FM broadcasting stations as an illuminator, and remodulates that signal based on the scatter radio principles [16]. The scatter radio tag uses backscatter FM modulation on an audio signal by switching the antenna between two loads. The reader captures the reflected signal, demodulates it and detects the frequency using periodogram-based Fourier analysis. This frequency corresponds to the measurement of the sensor. The measurements are sent to a base-station through adhoc network for remote supervision. This architecture, named ambient, can be considered as a special case of bistatic architecture as the illuminator is dislocated from the reader at a great distance. An example of the setup is shown in Fig. 4.1.
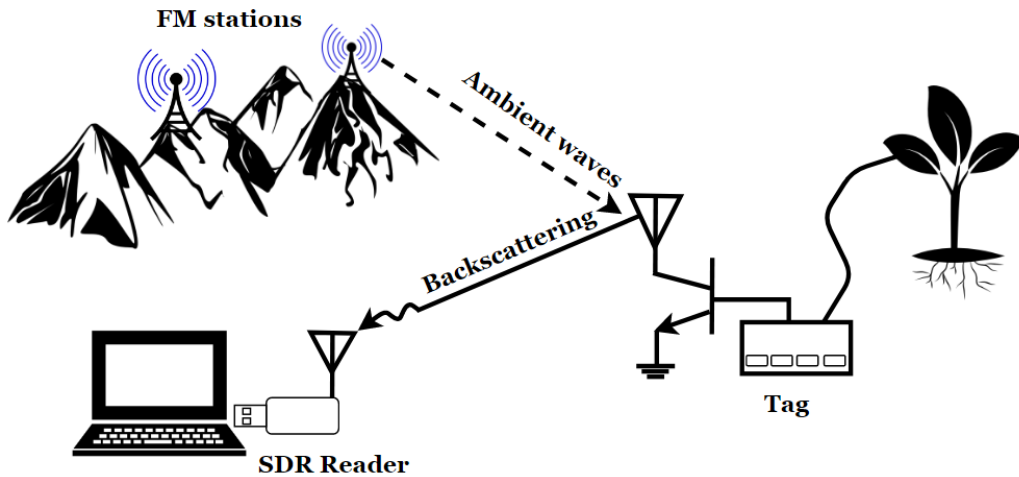

Figure 4.1: Ambient architecture.

4.1 Basic Theory

The signal transmitted from any FM radio station can be described from the equation [17]:

$$c_s(t) = A_s \cos\left(2\pi F_s t + 2\pi k_s \int_0^t \phi_s(\tau)d\tau\right), \tag{4.1}$$

where A_s , F_s is the carrier amplitude and frequency respectively, k_s is the modulator's frequency sensitivity measured in Hz/V. The term $\phi_s(\tau)$ corresponds to the audio information of the radio station. FM modulation index is given by $\beta_s = \frac{k_s max|\phi_s(t)|}{W}$, where W is the baseband bandwidth of $\phi_s(\tau)$.

The RF switch of the tag toggles between two different load coefficients:

$$\Gamma_i = \frac{Z_i - Z_a^*}{Z_i + Z_a}, \tag{4.2}$$

where Z_i corresponds to the tag load with $i \in \{0, 1\}$ and Z_a to the antenna impedance. The signal driving the switch with fundamental frequency F_{sw} can be expressed as:

$$x_{sw}(t) = A_{sw} \cos\left(2\pi F_{sw}t\right). \tag{4.3}$$

The FM modulated signal of the tag can be written in the following form:

$$x_{sw,FM}(t) = A_{sw} \cos\left(2\pi F_{sw}t + 2\pi k_{sw} \int_0^t \mu(\tau)d\tau\right), \tag{4.4}$$

which means that the signal driving the switch is modulated by $\mu(\tau)$, with fundamental frequency F_{sw}.

The modulated signal transmitted from the FM radio station $c_S(t)$ illuminates the tag and the backscattered signal is given by the equation:

$$\begin{aligned}
y_{bs}(t) &= \sqrt{\eta}c_s(t)x_{sw,FM}(t) = \\
&= \frac{\sqrt{\eta}A_{sw}A_s}{2} \cos\left(2\pi(F_s + F_{sw})t + \Phi_s(t) + \Phi_{tag}(t)\right) + \\
&+ \frac{\sqrt{\eta}A_{sw}A_s}{2} \cos\left(2\pi(F_s - F_{sw})t + \Phi_s(t) - \Phi_{tag}(t)\right),
\end{aligned} \tag{4.5}$$

where $\sqrt{\eta}$ is the scattering efficiency depending on the antenna characteristics and the chosen loads. The following abbreviations for Φ_{tag}, Φ_s are made:
$\Phi_{tag}(t) = 2\pi k_{sw} \int_0^t \mu(\tau)d\tau$, $\Phi_s(t) = 2\pi k_s \int_0^t \phi_s(\tau)d\tau$.

The equation [eq. 4.5] gives the sum of two FM signals at frequencies $F_s \pm F_{Sw}$ where the instantaneous frequency depends on $\phi_s(t)$ and $\mu(t)$. When the illuminating and the switching signals are FM, the backscatter results also to FM signal. The above phenomenon is called remodulation. This principle practically means that if we tune any FM receiver in frequency offset $\pm F_{sw}$ from the carrier frequency F_s of a radio station we can demodulate the backscattered signal as long as:

- the bandwidth of $\mu(t)$ is limited to the audio spectrum in between 20 Hz - 20 kHz or higher up to 53 kHz in case of stereo reception.

- at least one of $F_S \pm F_{sw}$ is within the FM band (88 MHz - 108 MHz).

- audio level of the backscattered demodulated tag signal is above a required threshold for successful demodulation.

The received audio information is the sum of the RF-tag's and radio station's demodulated signal $\mu(t) + \phi_s(t)$ where $\phi_s(t)$ corresponds to the audio information of the radio station, acting as interference in the reception of the desirable backscattered information $\mu(t)$.

4.2   Experimental Setup

The experimental setup consists of the backscatter sensor, the LimeSDR, the host PC that carries out the signal processing and a second computer as the base-station. Fig.4.2 presents the setup without the base-station. LimeSDR is tuned in FM band, captures the signal, transfers the data through USB3.0 to the host PC, which executes the signal processing that has been utilized through GNU-Radio software. After processing, the sensed information is transferred to the base-station. For this purpose, a WiFi adhoc network is implemented. The network takes advantage of a USB adapter following

he IEE-802.11 b/g/n protocols at 2.4 GHz and does not rely on any pre-existing infrastructures such as routers or access points. The communication is achieved with a server-client model under UDP protocol. The signal of the sensor is an analog signal, with a frequency that changes through a capacitance, according to the soil moisture. The frequency varies in range of 3.2 kHz to 700 Hz as the soil moisture increases.

Figure 4.2: Ambient reader experimental setup.

4.2.1 Reader Flowgraph

To capture the analog signal of the sensor, a FM receiver needs to be deployed [18]. At the next step, the periodogram-based Fourier analysis is used to detect the frequency of the signal. This process has been carried out with GNU Radio software environment and the blocks of the flowgraph are presented in this section analytically as shown in Fig.4.3.

LimeSuite Source (RX) block: This block represents the connection of the hardware and configures the LimeSDR receiver. It is tuned in FM band frequency ±300 kHz from the carrier of a radio station. The carrier is selected according to higher audio level. The configuration of the receiver is listed below:

- Center Frequency: 89.8 MHz.

- Sampling Rate : 1 MHz.

- Oversample: 32.

- NCO frequency: 0 (deactivated).

- Callibration Bandwidth:0 (deactivated).

- Channel A LNA path: LNAL.

- Analog Filter Bandwidth: 1.5 MHz.

- Digital Filter Bandwidth: 100 kHz.

- Channel: A.

- Antenna Port: RX1-L.

- Gain: 60 dB.

Low pass filter: Unnecessary frequencies of spectrum above 100 kHz are filtered out. Sampling rate has to be equal as to the previous block (1 MHz), in order to avoid bottlenecks in the flowgraph. As the flowgraph does not need to operate at the same sampling rate as the hardware, the output of the filter is decimated by a factor of 4, resulting in a sampling rate of 250 kHz.

WBFM Receive: This block demodulates a FM broadcast signal with a sampling rate of 250 kHz. The input is the downconverted complex baseband signal and the output is the demodulated audio signal.

Rational Resampler: The current block uses a ratio interpolation/decimation to change the sampling rate of the flowgraph. As the sound cards have specific sampling rate, and the audio signal bandwidth spectrum is limited (no need for 250 kHz), the rate is resampled to 48 kHz.

Audio sink: This module is connected to the sound card of the computer for debugging reasons. The audio signal of the sensor can be reproduced through it.

DC Blocker: This filter is used to remove the DC spike. Due to leakage reasons, a DC spike is observed, resulting in an error of detection towards the peak value of the frequency as pointed at the DC. **Stream to vector:** Converts the bit-stream to a subset of vectors. Practically this block slices the audio signal to segments, for further analysis.

FFT: This block computes the fast Fourier transform of the audio signal. The size of the FFT window has $N = 2048$ samples and the sampling rate is $F_s = 48$ kHz. The resolution of the FFT analysis is $\frac{F_s}{N} = 23.43$ Hz.

Vector to stream: Opposite functionality of stream to vector block. Converts the stream of vectors to a stream of bits.

Complex to Magnitude squared: The magnitude of the Fourier analysis squared is calculated for the completion of the periodogram-based analysis.

Keep M in N: Keeps the samples that correspond to the positive semi-axis of the spectrum.

Argmax: Accepts a vector as input and detects the maximum value and the index of it. The index is used to find the corresponding position on frequency axis.

Null Sink: Bit bucket for unwanted bit-stream.

Get Maximum Frequency: Custom block for the frequency axis creation. From Nyquist-Shannon sampling theorem [19], it is known that sampling frequency F_s should be at least equal or greater than twice the bandwidth B of a signal, $F_s \geq 2B$. Consequently, the bandwidth is less or at least equal to $F_s/2$. Therefore, the semi-axis of the positive frequencies will be $[0, F_s/2]$, where F_s is the sampling frequency is set to 48 kHz based on the flowgraph. The frequency vector is equally spaced with the number of samples of the FFT in the positive semi-axis. Based on the above, corresponding frequency can be detected with the index of the maximum peak value as input from the previous block.

Repeat: Repetition of each result through the UDP socket, counterbalancing possible packet corruption.

UDP sink: Writes the results to a UDP socket. This block is used to transfer the sensed information to the remote base station through the adhoc WiFi network.
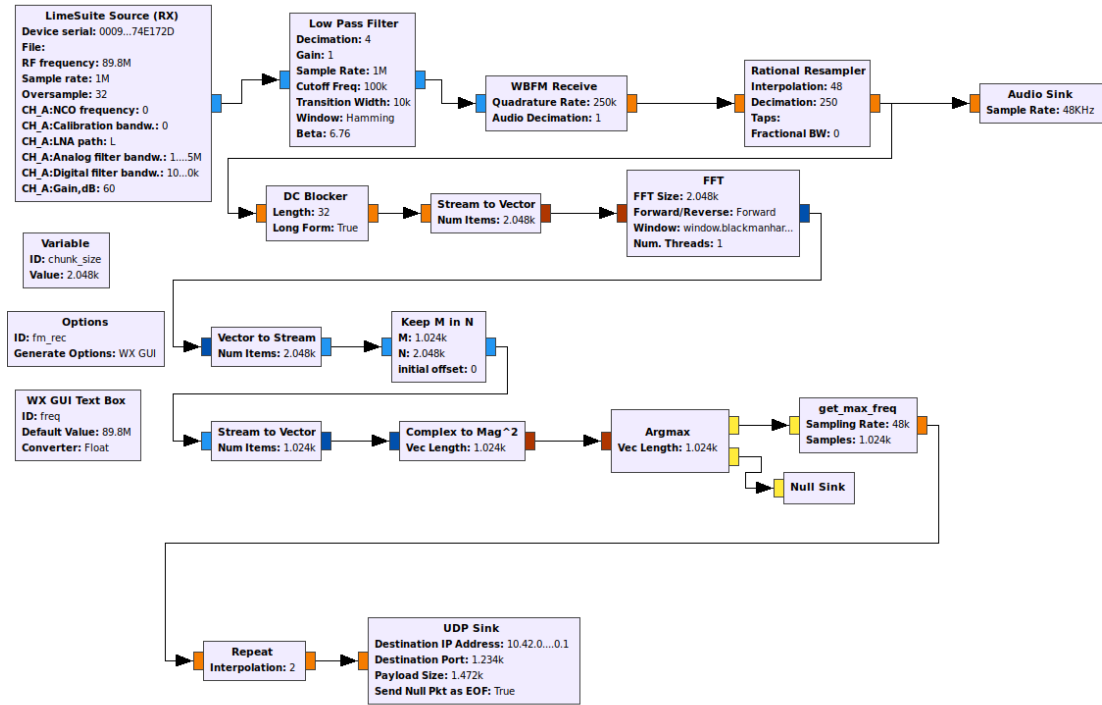
Figure 4.3: GNU Radio flowgraph.

4.2.2 Adhoc Network

A wireless adhoc network is implemented for peer to peer communication between the reader and the base station for range coverage extension and remote supervision of the sensor measurements. Each node of the network has a unique IP address for the packet transmission through sockets. The reader node represents the client sending the sensed information and the base station simulates the server receiving tha data. In order to maximize the distance between the reader and basestation, the rate of the WiFi USB adapter is set to the minimum value, equal to 1 Mbps. The UDP protocol is used for packet transmission. This protocol is unreliable compared to TCP, as there is no guaranteed delivery and a datagram packet may become corrupted or lost during transmission. However, a non-handshake protocol is preferable in achieving greater range coverage between two nodes. Each packet is repeated twice to counterbalance possible packet loss.

Chapter 5

Experimental Results

5.1   Monostatic Receiver Results

Two experiments are conducted to measure the range coverage of the LimeSDR receiver in a monostatic architecture. In the first experiment, the Tx port of LimeSDR is connected directly to the antenna. The output transmission power of LimeSDR with maximized gain at the transmit chain, is experimentally measured from the board port with value equal to 2 dBm. The achieved communication range is 9.40 meters, as it is shown in Fig.5.1. In the second experiment the Tx port of the LimeSDR is connected to an amplifier before the antenna. The new output transmission power of the carrier emitter is measured at 23.9 dBm. The new communication range achieved with the amplifier is equal to 13.7 meters.
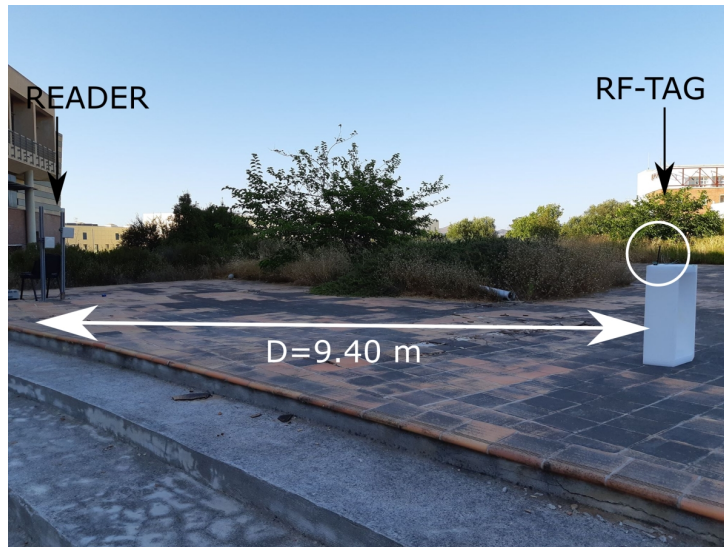

Figure 5.1: Maximum range without amplifier.

5.1.1 Observations

Without amplifier: Measurements directly from the transmit port of the board indicated some non-linearities, probably produced from the electronic components of the board. The measurement of spectrum analyzer is presented in Fig. 5.2.
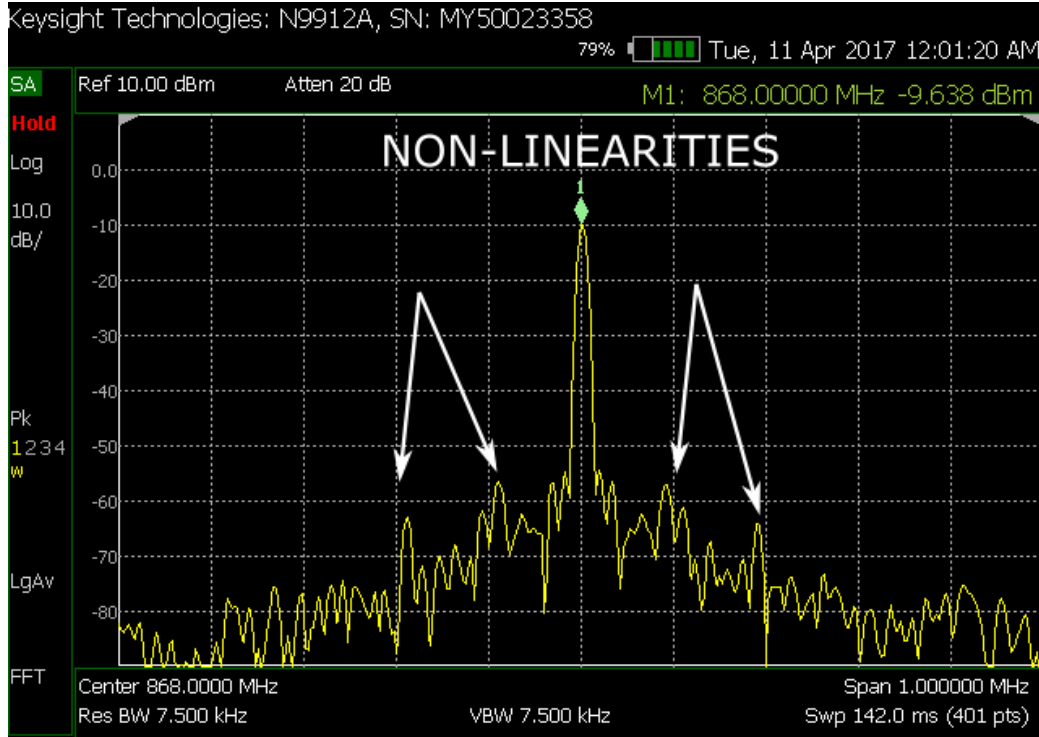

Figure 5.2: Constant wave without amplifier. Peak at 2 dBm (-9 dBm indication + 11 dBm external attenuator).

With amplifier: The use of the amplifier did not extend the range as much as expected. Besides the constant wave, non-linearities are also amplified, which is feasible. These unwanted peaks act as phase noise for the receiver because the antennas stand close in a monostatic architecture. Consequently, as the tag-to-reader distance increases, the SNR ratio is decreased and symbol detection is not so efficient. The amplified non-linearities are shown in Fig. 5.3.
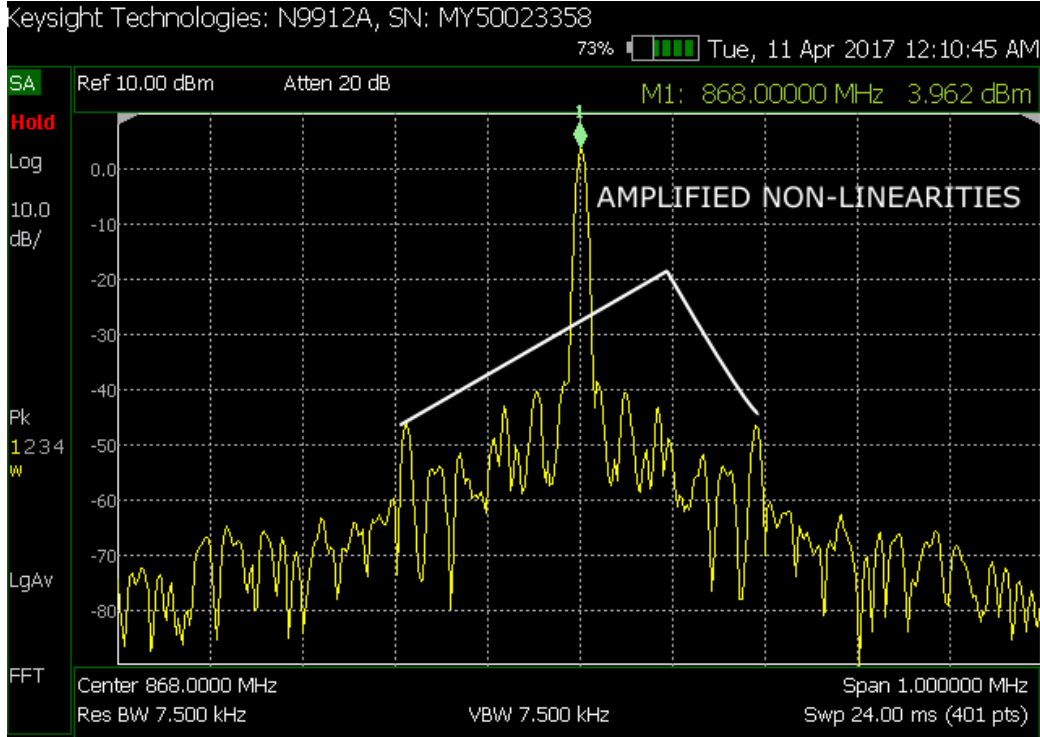
Figure 5.3: Constant wave with amplifier. Peak at 23.9 dBm (3.9 dBm indication + 20 dBm external attenuator).

5.2 Ambient Receiver Results

The frequency of the produced signal by the sensor was experimentally measured with a frequency counter on the switch of the circuit. This value is used as reference for the calculation of the root mean square error of the reader's results.

$$RMSE = \sqrt{\Sigma_{i=1}^{N}\left(\frac{(x_i^{pred} - x_i^{ref})^2}{N}\right)}. \tag{5.1}$$

5.2.1 Sensor to Reader Range

Experiments for the root mean square error versus the distance between sensor and reader were conducted. As presented in Table 5.2.1, the threshold distance, where the reader could receive the signal of the sensor, is 7 meters,

while the RMSE is less than 200 Hz.

Distance (m)	RMSE (Hz)
1	4.41
2	12.75
3	27.02
4	40.76
5	88.35
6	130.95
7	162.63
8	592.31
9	585.38
10	1801.12

Table 5.1: RMSE vs Distance.

5.2.2 Observations

A smartphone with embedded FM receiver is used to compare the range
where the audio signal of sensor could be received. The smartphone achieved
a greater range, due to the dedicated hardware, which implements the FM
demodulation and higher quality analog filters that absorb less thermal noise.
Practically, other factors that could affect the range are the distance from
the source of the illuminating signal and the antenna used on the scatter
sensors. In the specific experiment, the source of the illuminating signal is
approximately 7 kilometers away and a monopole wire is used as the antenna
of the sensor.

5.2.3 Reader to Base-station Range.

The maximum distance between the reader and the base-station is heavily
depended on the network infrastructure. In the current implementation as
mentioned in section [4.2], the only network support device is the WiFi USB
adapter. The range is measured for both TCP and UDP protocols. Up

to 70 meters, both protocols performed sufficiently enough. Beyond that point, the TCP handshake procedure stopped, while the UDP equivalent was degraded, but packets were received. Longest distance achieved with UDP protocol before the complete lost of connection was approximately 146 meters as depicted in Fig. 5.4.

Figure 5.4: Adhoc network communication range.

Chapter 6

Conclusion

This work focused on the implementation of backscatter radio applications for environmental sensing with the use of the LimeSDR board. Two readers for digital and analog data were implemented. Signal model, experimental setup and results were analytically presented for both applications. In the first application, the performance of LimeSDR was evaluated with range measurements, as a compact reader (illumination and reception of the RF-tags) based on monostatic architecture. Similarly, for ambient architecture, both the LimeSDR to scatter sensor distance and the root mean square error (RMSE) were measured to evaluate the reliability of the reader. Hardware and configuration of the LimeSDR board is also presented. Additionally, a WiFi adhoc network was designed to extend the range capabilities for both readers. LimeSDR is a powerful board with great features, serving a variety of applications. The price of the LimeSDR makes it suitable for low-cost implementations of wireless sensor networks, as the total expenses drop significantly. In conclusion, this work contributes to further cost optimization of wireless sensor networks applications of current research.

6.1 Future Work

The functionality of LimeSDR was constrained to half-duplex operation (1 transmit & 1 receive channel). It could prove challenging to exploit both channels of the transceiver for multi-hop wireless sensor network applications. Specifically, the first channel could be used for illumination of the tags and reception of the backscattered signal (monostatic architecture), and the second channel could be used for the communication between different Lime devices for data transferring. This could extend the range coverage and

improve network management. As far as the current work is concerned, fine-tuning the configuration parameters of the LimeSDR board could lead to further optimization of the systems.

Bibliography

[1] MyriadRF, "Limesdr hardware description." [Online]. Available: https://myriadrf.org/news/limesdr-made-simple-part-1/

[2] ——, "Limesdr hardware description." [Online]. Available: https://wiki.myriadrf.org/LimeSDR-USB_hardware_description

[3] ——, "Lime sdr functional block diagram." [Online]. Available: https://wiki.myriadrf.org/LimeMicro:LMS7002M_Datasheet

[4] G. Vannucci, A. Bletsas, and D. Leigh, "A software-defined radio system for backscatter sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2170–2179, Jun. 2008.

[5] J. Kimionis, A. Bletsas, and J. N. Sahalos, "Increased range bistatic scatter radio," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1091–1104, Mar. 2014.

[6] P. N. Alevizos, K. Tountas, and A. Bletsas, "Multistatic scatter radio sensor networks for extended coverage," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4522–4535, Jul. 2018.

[7] Wikipedia, "Software define radios." [Online]. Available: https://en.wikipedia.org/wiki/Software-defined_radio

[8] L. Microsystems, "Limesdr product." [Online]. Available: https://limemicro.com/products/boards/limesdr/

[9] LimeMicrosystems, "Lms7002m transceiver datasheet." [Online]. Available: https://limemicro.com/app/uploads/2017/07/LMS7002M-Data-Sheet-v3.1r00.pdf

[10] GnuRadio, "Gnuradio software." [Online]. Available: https://www.gnuradio.org/

[11] MyriadRF, "Limesuite software." [Online]. Available: https://wiki.myriadrf.org/Lime_Suite

[12] ——, "Soapylms7 bindings." [Online]. Available: https://github.com/myriadrf/LimeSuite/tree/master/SoapyLMS7

[13] ——, "Gnuradio plugin for limesdr." [Online]. Available: https://github.com/myriadrf/gr-limesdr

[14] K. Tountas, "Implementation of frequency division multiple access digital backscatter sensor netwok," Master's thesis, Technical University of Crete, Oct. 2014, supervisor A. Bletsas.

[15] MyriadRF, "Limesdr configuration through gr-limesdr plugin." [Online]. Available: https://wiki.myriadrf.org/Gr-limesdr_Plugin_for_GNURadio

[16] G. Vougioukas and A. Bletsas, "Switching frequency techniques for universal ambient backscatter networking," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 2, pp. 464–477, Feb. 2019.

[17] ——, *Smartphone Reception of μWatt, m-km Range Backscatter Resistive/Capacitive Sensors with Ambient FM Remodulation & Selection Diversity*, N. B. Carvalho, Ed. Elements Series, CAMBRIDGE UNIVERSITY PRESS, Mar. 2018, submitted.

[18] MyriadRF, "Fm receiver example." [Online]. Available: https://github.com/myriadrf/gr-limesdr/blob/master/examples/FM_receiver.grc

[19] Wikipedia, "Nyquist shannon sampling theorem." [Online]. Available: https://en.wikipedia.org/wiki/Nyquist\OT1\textendashShannon_sampling_theorem