TECHNICAL UNIVERSITY OF CRETE
ELECTRONIC AND COMPUTER ENGINEERING DEPARTMENT
TELECOMMUNICATIONS DIVISION

Design and Implementation of Backscatter Links with Software Defined Radio for Wireless Sensor Network Applications

by

John Kimionis

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

ELECTRONIC AND COMPUTER ENGINEERING

November 2011

THESIS COMMITTEE

Assistant Professor Aggelos Bletsas, *Thesis Supervisor*
Assistant Professor George N. Karystinos
Professor Athanasios P. Liavas

Abstract

Backscatter radio is an appealing communication scheme, common in radio frequency identification (RFID), which can be used in wireless sensor networks (WSNs) for environmental sensing. A centralized *reader* transmits a carrier, which is reflected with modulated information by antenna-equipped *sensors*. The reader extracts each sensor's information from the reflected signals and thus, a sensor does not utilize an active radio. Therefore, a sensor demands significantly lower energy and costs much less, compared to conventional WSN technologies (e.g. 802.15.4/ZigBee). However, intelligent (i.e. non-trivial) design for the sensors and the reader is required.

In this thesis, a complete backscatter system is designed and implemented, by utilizing communication, radio, circuit, RF electronics, and signal processing theory. A custom backscatter sensor is built from first principles, along with a reader, which is implemented with commodity, low-cost software defined radio (SDR). Backscatter links are tested, demonstrating their inherent tradeoffs in terms of range, bit-error-rate (BER) and multiple access. Theoretical results match simulation and are experimentally validated with the constructed testbed. This work is a proof of concept for ultra-low cost and low power wireless communication by means of backscatter and low-cost SDR technology. The implemented testbed serves as a practical and efficient solution for backscatter radio research.

Thesis Supervisor: Assistant Professor Aggelos Bletsas

Acknowledgements

Here, I would like to thank the people that supported me at all aspects throughout this work and the writing of this thesis.

First of all, my parents and my sister who always supported me in all ways. Their extensive encouragement has been of great importance. I want to thank them for everything they have given to me.

Then, my friends and the people who love me. I want to thank them for the valuable moments we have enjoyed together during this full-time working period. The patience and encouragement of some of them have really been valuable to me. :)

Finally, I would like to thank my professors, and especially my advisor Dr. Aggelos Bletsas, who has been a great source of inspiration and motivation for research. I was fortunate enough to meet him in the fifth year of my undergraduate studies and work together since then. He really persuaded me and other members of his group that quality work can be done in a Greek university. Research can be fun, and every single idea counts. Everything can be built up from scratch, after hard work; and this is the most important fact in such a difficult era for this country.

To a special person that used to welcome me with the words:
"Hello Mr. Engineer..."

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ACK	Acknowledgement	
ADC	Analog to Digital Converter	
BER	Bit Error Rate	
BPSK	Binary Phase Shift Keying	
CW	Continuous Wave	*Unmodulated carrier*
DAC	Digital to Analog Converter	
DC	Direct Current	*Signal with a frequency of 0 Hz*
DSP	Digital Signal Processing	
DTV	Digital Television	
EPC	Electronic Product Code	
FDM	Frequency Division Multiplexing	
FDMA	Frequency Division Multiple Access	
FEC	Forward Error Correction	
FIFO	First In First Out	
FM	Frequency Modulation	
FM0		*Biphase-space line coding*
FPGA	Field Programmable Gate Array	
FSK	Frequency Shift Keying	
GND	Ground	
GPIO	General Purpose Input/Output	
GSM	Global System for Mobile Communications	
I/Q	In-phase/Quadrature	
ISA	Instruction Set Architecture	
ISM	Industrial, Scientific, Medical	*RF band*
LED	Light Emitting Diode	
MAC	Medium Access Control	

MCU	Microcontroller Unit	
MDD	Minimum Distance Detector	
ML	Maximum Likelihood	
MRC	Maximum Ratio Combining	
MSK	Minimum Shift Keying	
NA	Network Analyzer	
NF	Noise Figure	
OOK	On Off Keying	
PCB	Printed Circuit Board	
PDF	Probability Density Function	
PSK	Phase Shift Keying	
RCS	Radar Cross Section	
RF	Radio Frequency	
RFID	Radio Frequency Identification	
RH	Relative Humidity	
RN16		*16-bit random number*
SDR	Software Defined Radio	
SMA	SubMiniature version A	*Antenna connector type*
SMT	Surface MountType	
SNR	Signal to Noise Ratio	
UART	Universal Asynchronous Receiver/Transmitter	*Serial interface*
UHF	Ultra High Frequency	*RF band*
USRP	Universal Software Radio Peripheral	
VDD		*Digital Supply Voltage*
WSN	Wireless Sensor Network	

Chapter 1

Backscatter and RFID: Wireless Transmission without Radiation

The roots of transmission of information without radiation hold from the era the *radar* was invented. The first paper on the use of backscatter radio was published in 1948 [1] expanding the operation of radars to other systems that would modulate signals by reflecting them towards their source. Today, the most common use of the principles of backscatter is in radio frequency identification (RFID) applications, where electronic product codes (EPC), able to be read in a RFID *reader's* electromagnetic field, tend to replace the classic barcode; the latter requires to be (literally) seen from a close distance to be decoded, setting it unsuitable for some applications. However, more applications incorporating backscatter technology have emerged recently than just identification, with one of the most interesting ones being its use in wireless sensor networks (WSNs) as a cost- and energy-efficient communication scheme.

1.1 Backscattering vs. Active Transmission

The main principle of backscatter radio is that modulation on a transmitter, named the *tag*, is achieved by controlling how a carrier wave arriving at an antenna is reflected back. By 'how' we mean that the signal's amplitude, or phase, or both are changed in such a way that can be detected by a receiver (typically called the *reader* in backscatter radio). The carrier that arrives at the tag and its reflection is modulated (by the tag) is actually

transmitted by the one who also receives the backscattered signals. So, the 'master' in a backscatter link is the reader, which transmits a carrier in order to hear what the tags have to say. Without the carrier transmission, no backscatter communication can be achieved, contrary to active radios, where anyone can transmit and be heard anytime. Active radios are standalone devices which employ their own oscillator for carrier generation, followed by a modulator which changes the carrier's characteristics (amplitude, phase, frequency) according to the data to be transmitted, and finally a power amplifier to strengthen the modulated signal enough, to be finally radiated from the transmitting antenna. Their design is much more complex than backscatter tags, and these devices are energy demanding because of the active components they use to create and amplify signals. On the contrary, a backscatter tag, being a 'dumb' transmitter which cannot work without a (more complex) reader follows a very simple design for its RF part.

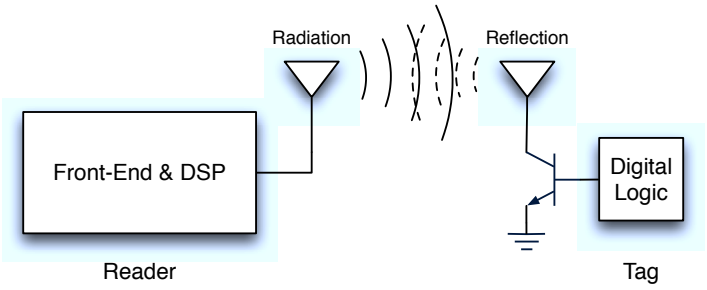

Figure 1.1: Monostatic backscatter reader-tag system.

A tag does not need to employ an oscillator for frequency generation, as the carrier is already there from the reader who initiates the communication. The antenna, which has a nominal impedance, is connected to a load. According to the value of the load, a portion of the power appearing at the antenna's terminals will be consumed on the load and the remaining will be reflected back from the antenna. If the value of the load changes, a different portion of power (say lower than the first) will be absorbed by the load, and the reflected power will be larger. Therefore, the simplest paradigm would be that the first load value is chosen so that all power induced on the antenna is absorbed from it (the load), and the second is chosen so that all power will

be reflected back to the antenna [2]. This would result in an amplitude modulation effect, as the reader would detect the different backscattered power levels. However, things are more complex, as by altering a load value, not only the amplitude changes, but also the phase of the backscattered carrier. Thus, different modulation schemes can be implemented, like Phase Shift Keying (PSK). The selection of load values for backscatter tags is a field of active research, employing knowledge of microwave theory, circuits, and communications.

A reader can follow a *monostatic* architecture, like the one shown in Fig. 1.1, where carrier generation and tag signal reception is done on the same box. Commonly, a monostatic reader is a homodyne radio, which uses the same oscillator both for carrier transmission and for tag signal demodulation. Most commercial RFID readers follow this scheme; it is a well-packed solution with convenient signal processing, as no frequency offsets are present between the transmitting and receiving part. However, sometimes a *bistatic* architecture is preferred for several reasons. The carrier generator and the receiver of the reader are two separate boxes, which can be either colocated or dislocated (Fig. 1.2). This may reduce the issue of transmit power leakage to the receiving part, which is a common problem in monostatic readers [2].

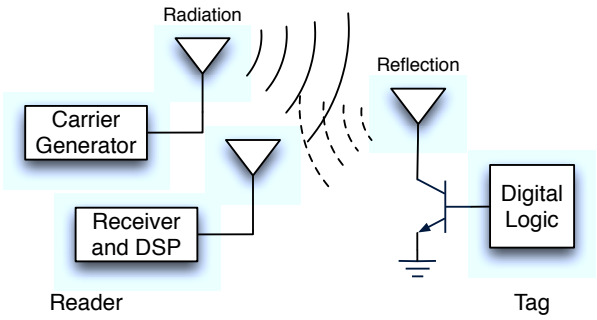

Figure 1.2: Bistatic backscatter reader-tag system.

1.2 RF tags - Categories and Applications

RF tags can be distinguished into two main categories, as far as the type of information they transmit is concerned:

1. **RFIDs**, when they are used for identification of an object by a product code. Usually, the information backscattered from such tags is static and one-time-stored (or may change rarely under circumstances).

2. **RF sensors**, when they are used to sense a (usually) time varying environmental quantity (e.g. humidity, temperature, gas emissions, sound level, etc) and backscatter a digitized form of that quantity. The information transmitted is dynamically changed.

A significant categorization of RF tags is according to their power source:

1. **Passive tags** use a rectified portion of the reader's transmitted carrier power to power their digital logic, and stay alive as long as a reader's electromagnetic field is present. The uplink communication is achieved by scattering a portion of the induced carrier power back to the reader.

2. **Semi-passive tags** are energy-assisted units, that use a battery or an energy harvesting source to power their digital logic, but still use backscattering as a communication scheme.

3. **Active tags** are essentially active transmitters that use battery power both for their digital logic and for the transmission of RF signals towards the reader by radiation. They utilize a common radio with an oscillator, a mixer and a power amplifier.

The tag's power source determines the communication range it can achieve. A passive tag's range is limited by the reader-to-tag distance required to harvest adequate power to wake the tag up, even though the *uplink* (i.e. tag to reader) communication range may be longer (when the reader is of high sensitivity). This results in short ranges of a few meters. This is not the case with semi-passive tags, which have a dedicated power source and whose range is only limited by their backscattering *efficiency*, capable of getting

up to some decades of meters. Active tags, utilizing active transmitters and higher capacity batteries than the semi-passive ones, are only limited by their power amplifiers' gain and consumption, making them suitable for long communication ranges of hundreds of meters.

Usually, the type of information an RF tag transmits is tightly coupled with its power source. For example, in supply chain applications, where a fixed reader interrogates tags on boxes for a product code, the common practice is the use of passive tags, as the information is of interest only at the time the box is interrogated. After that, the tag may 'go to sleep'. Also, since the information is static (just a fixed series of bits), there is no need for complex digital logic, and thus no need for large amounts of power. In that case, RF power harvesting is sufficient, considering the application's low range requirements. Moreover, passive tags are cheap, compared to semi-passive, and the (more expensive) active ones. Below, some common applications for specific types of tags are presented.

- **Passive Tags**: Product identification in supply chain, documents identification, human authentication.
- **Semi-passive Tags**: Backscatter networks, electronic toll collection.
- **Active Tags**: Long range sensor networks.

Chapter 2

Backscatter Sensor Networks

In this chapter, we introduce the main concepts of backscatter sensor networks and the differences between them and classic wireless sensor networks. Prior art in the field is presented, plus an experimental setup developed throughout this thesis, for research and experimentation on Backscatter links and networks.

2.1 Sensing for Precision Agriculture

The main motivation that lead to this work was water saving in agricultural applications. Precision agriculture, irrigation scheduling, and plant monitoring in general, highly rely on soil wetness observation. To achieve this, a large infrastructure of sensing units has to be placed on a field or in a greenhouse, up to one per plant for example. However, in most cases, wiring hundreds of sensors to a measurement station is not feasible due to spatial limitations, while such a large population of wireless transceivers with sensors would be of high cost.

2.2 From Wireless Sensor Networks to Backscatter Networks

Recently, a lot of commercial platforms have emerged for agricultural sensing, exploiting wireless communication schemes (e.g. ZigBee) and employing multi-hop or multiple access network architectures. The great downside of these platforms is their cost, which is a big limitation if ultra-high sensor density is required for the application. Indicative prices for one commercial sensor node vary on the range of \$100–\$200. Custom solutions are proven

Figure 2.1: Modern greenhouses are in need of constant monitoring.

to be a lot more cost-effective (e.g. iCube [3]), but for the application under investigation, the cost has to be reduced to the order of a few dollars, or less.

Power consumption plays a major role on the overall efficiency of a sensor node. Taking into account that market-available batteries have not made any great progress throughout the last ten years in terms of their capacity, sensor nodes have to be as low energy-demanding as possible. The power consumption of current wireless sensor nodes is shown to be determined mainly by their radio modems, as active parts like the power amplifiers employed for transmitted signal amplification require a non-negligible amount of energy. Moreover, at their receiving part, complexity and energy demands are increased due to sophisticated decoding, forward error correction (FEC), etc.

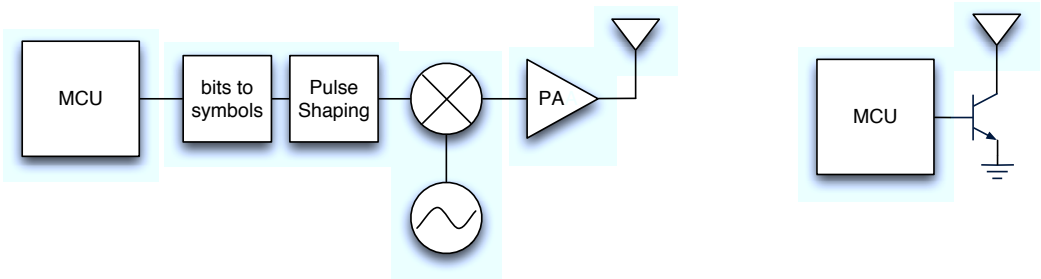

Figure 2.2: Active transmitter (left) vs. Semi-passive RF tag (right).

One can observe that there is no existing technology incorporating all the requirements (low cost, low power, small form factor). Even if portions of the

existing technologies can be made cost-effective (e.g. radio transceivers), they have not shown to be energy efficient yet. Thus, a whole new approach to the problem is required; that being the shift of complexity from the transmitters (sensor nodes) to the receiver (network main node/gateway). In its simplest form, a sensor node only transmits information according to what it has sensed. Respectively, the network gateway acts as a sink for information collected from all nodes. This leads to a network architecture of lots of relatively simple nodes, with ultra-low complexity RF front-ends, and a smart receiver, which processes all information regarding the plants on a field.

Backscatter communication is an ideal scheme for this network architecture; sensor nodes can be in the form of semi-passive tags, whose RF front-end is very simple compared to the complex active transmitters, as already described in Chapter 1. Moreover, the energy required for the RF part is eliminated, as the latter is consisted by a single transistor. Because the tag is semi-passive, the range is extended compared to simple passive tags; the latter achieve ranges on the order of 2–3 meters. The network gateway will be in the form of a backscatter/RFID reader, which will be software-defined in order to provide the flexibility needed to handle several modulation schemes according to the network's needs. More on the tag design and the software defined reader is covered throughout the next two chapters of this thesis.

2.3 Prior Art in the Field

Prior art in the field of backscatter sensor networks includes a demonstration of a one-to-one backscatter radio system [4]. One semi-passive node 'talks' to a custom software defined reader by modulating and scattering back the reader's carrier. The work is a proof of concept for backscatter networks and provided the motivation for expansion to multiple nodes in this thesis. Theoretical work has also been done on the sensor interference quantification in such networks, where multiple carrier frequencies are employed for the network's uplink [5].

On the backscatter tag side, previous work on design of battery-assisted RFID sensors for wireless sensor networks has been done [6], showing how

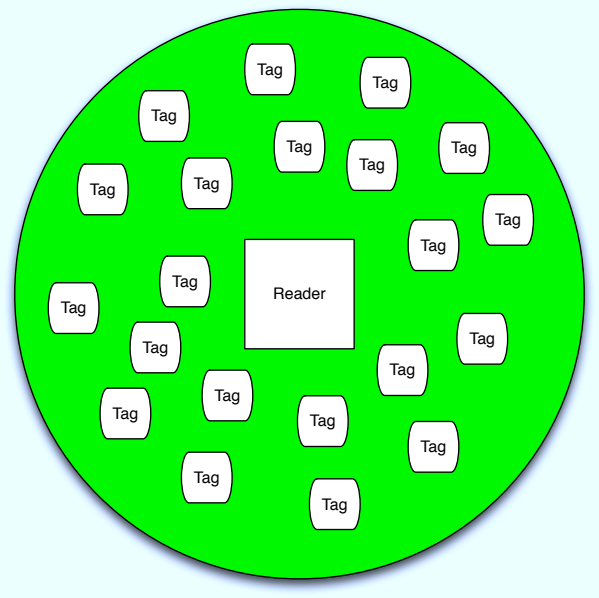

Figure 2.3: Backscatter field.

RFID tags with embedded sensors can lead towards a new form of sensing. Design considerations for power harvesting from sources other than batteries and their efficiency can be found in recent literature. Examples are solar energy [7], kinetic energy [8], and electromagnetic energy [9]. On the RF part, analysis of the design constraints for backscatter tags has also been done [10]. Design considerations with respect to efficient backscatter communication are proposed, in terms of range maximization and bit error rate (BER) performance. The results of that work have been used throughout this thesis, and laboratory measurements based on that work's theoretical findings have been made in the thesis's experimental part. A complete link budget analysis between a tag and monostatic/bistatic readers has been done in [11]. Experimental measurements for a tag's maximum range have been done in this thesis, with respect to some of that work's findings.

Finally, on the reader side, a Generation 2 RFID Standard compatible software defined reader has been demonstrated, with the use of USRP hardware and GNU Radio software processing blocks [12]. That work's concepts are adapted in this thesis, as far as the hardware platform is concerned, but

signal processing in this thesis is taking place on MATLAB environment with custom scripts written from the ground up, making the reader more flexible and thus supporting additional modulation schemes than those specified in Generation 2 Standard [13].

2.4 Experimental Setup for Research on Backscatter Links and Networks

Here we present a complete bistatic backscatter system, developed and used throughout this thesis, for research and experimentation on backscatter links and networks. The backscatter setup consists of both commercial laboratory equipment and custom built hardware and software. In the next two chapters, the use of the equipment is fully explained, with emphasis on the tag and reader parts.

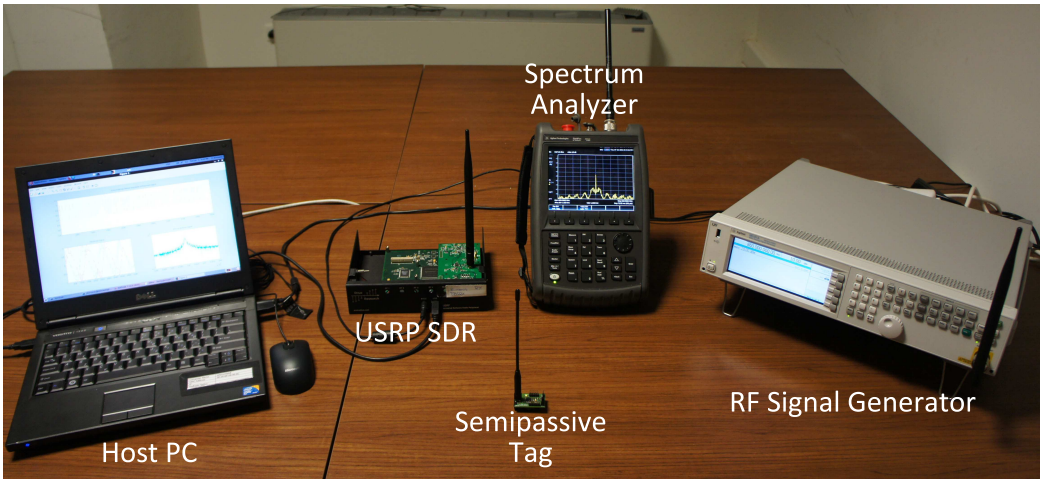

Figure 2.4: Experimental setup.

2.4.1 System Architecture

RF Signal Generator

The signal generator is used to transmit a constant sinusoid at a carrier frequency selected, for making backscatter communication possible. The carrier

frequencies are selected in the unlicensed ISM UHF Bands (865–868MHz for Europe and 902–928MHz for USA/Canada).

- Model: Agilent N5181A.
- Frequency Range: 100kHz - 6GHz.
- Max Output Power: +30dBm.
- Antenna: 3dBi omnidirectional.

RF Spectrum Analyzer/Network Analyzer

The spectrum analyzer is used as a precise test/debug unit for signals in the frequency domain. Also, range measurements described later are made possible by observing the carrier's and backscattered signals' power versus the noise power.

The network analyzer mode is used for RF front-end measurements. RF transistors' performance is characterized as a function of their reflection coefficients in on or off states. Details on RF measurements take place in Section 3.2.

- Model: Agilent FieldFox N9912A.
- Frequency Range: 2MHz - 6GHz.
- Capabilities: Spectrum Analysis / 1-port and 2-port Network Analysis / Cable Testing.

Semi-passive tag

The semi-passive tag is a full custom design and implementation in the context of this thesis. Chapter 3 is dedicated on the design considerations and implementation details. All experiments throughout this work are based on this tag.

- Model: Full custom, built in Telecom Lab, ECE, Technical University of Crete.

- MCU: SiLabs C8051F320.
- RF transistor: (One of) Agilent AT-32033 / NXP BFS17NTA / CEL NE68033-A.
- 3V Coin Battery (CR-2032) holder & Sensor Connectors.

Software Defined Reader

The reader consists of the software defined radio (SDR) hardware platform used to capture, down-convert and digitize on-air signals, and the software platform used to transfer the digitized samples to the host PC and process them on MATLAB. A detailed description of the whole reader system is on Section 4.1 of this thesis. The SDR hardware and the processing software are hosted on a mainstream laptop with modest capabilities.

- Software Defined Radio Hardware: Ettus Research Universal Software Radio Peripheral (USRP1) with RFX900 UHF front-end.
- Software Defined Radio Software: GNU Radio.
- Signal Processing Software: Custom software on Mathworks MATLAB environment.
- Host PC: Dell Vostro 1320 Laptop (Intel Core 2 Duo 2.53GHz, 1GB RAM).
- Operating System: Ubuntu Linux 9.10.

2.4.2 Limits on Maximum Range

Complete link budget analysis for backscatter radio with several reader configurations (monostatic, bistatic colocated, bistatic dislocated) has been made in [11], taking into account several factors of the wireless channel and antennas, like path blockages, antenna polarization mismatch, etc. Although these are important findings, most of the factors studied are difficult to be measured individually and their measurement has not been the priority of

this thesis. However, an empirical metric has been used for estimating a maximum achievable range with the instrumentation presented, which is the observation of the backscattered power in a real outdoor environment.

Experimental measurements of maximum range for the backscatter setup were made using a spectrum analyzer for backscattered power versus noise floor power observation. The field test was done on a garden full of tall, messy grass, where the signal generator was located at the field boundary and the spectrum analyzer (and software-defined reader) was moved away from the generator, until an estimation of the backscattered signal-to-noise ratio (SNR) reached a threshold of 6dB. The tag used for reference lied between the generator and the analyzer, and was set to continuously flip between two frequencies, leading to backscattering of two subcarriers, whose power was compared with the noise power. In Fig. 2.5, the received spectrum is shown, where the carrier peak can be seen, plus two subcarrier peaks corresponding to the two tag frequencies. The power ratio of either subcarrier versus the noise floor is ∼6dB.

Two scenarios were examined. In the first the tag was near the signal generator, thus inducing as much carrier power as possible, and in the second it was set in the middle of the generator–analyzer distance. The measurement results are shown in Table 2.4.2. It can be seen that for 30dBm carrier power and the tag being near the generator, the range can exceed 100 meters, while for a generator to tag distance of 25 meters, the uplink range is about 25 meters. The measurement results show that the larger the amount of induced carrier power is, the longer the range that can be achieved. This holds for a fixed *scattering efficiency*, which is defined as the ratio between reflected power and total induced power at the tag. It can be seen that maximization of the tag's scattering efficiency itself can lead to maximization of the achievable range. These experimental findings partially verify the theoretical work in [10].

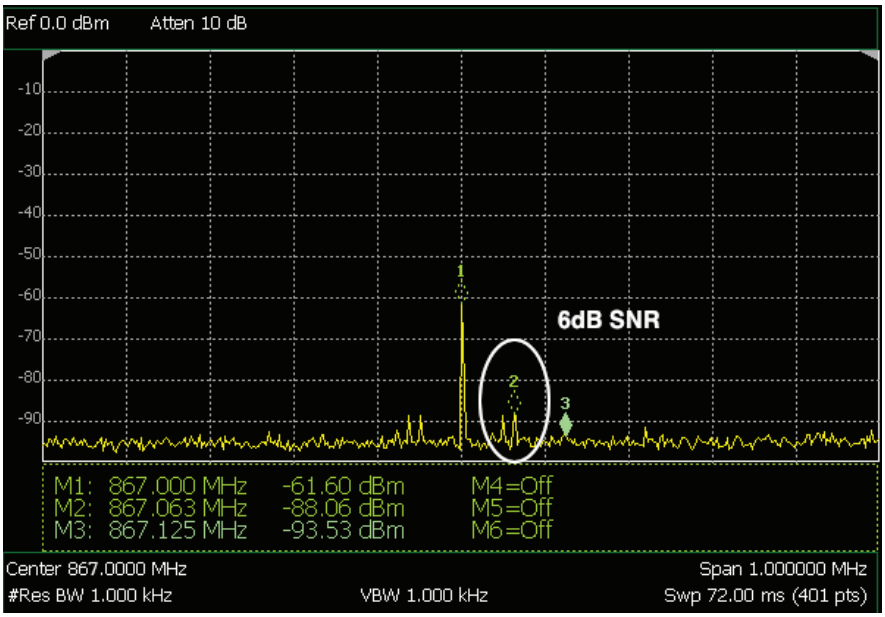

Figure 2.5: Observation of subcarrier power level versus noise power level.

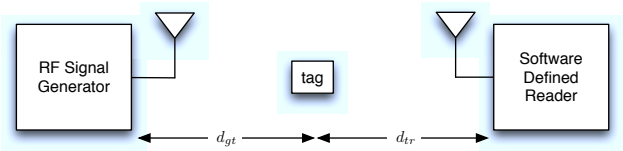

Figure 2.6: Bistatic dislocated architecture: RF signal generator is away from receiver (reader) and tags lie between them.

Generator to Tag distance d_{gt}	$0.1m$	$25m$
Tag to Receiver distance d_{tr}	$> 100m$	$25m$
Tag bitrate / Generator TX power	10bps @ 30dBm	10bps @ 30dBm

Table 2.1: Range measurements.

Chapter 3

Semi-passive Backscatter Tag Design

Tags are the piece of hardware which are attached to each plant, monitoring its microclimate by sensing important parameters like soil moisture, ambient temperature, etc. In this chapter, we present the design considerations followed to build a custom semi-passive tag capable of sensing and backscattering data towards the network's reader. We cover the hardware design, the RF part and how it affect's the tag's efficiency, the sensor circuitry, and the software that controls all tag actions. Starting from the design considerations for a 'classic' WSN node, we expand these considerations to the concepts of backscatter nodes.

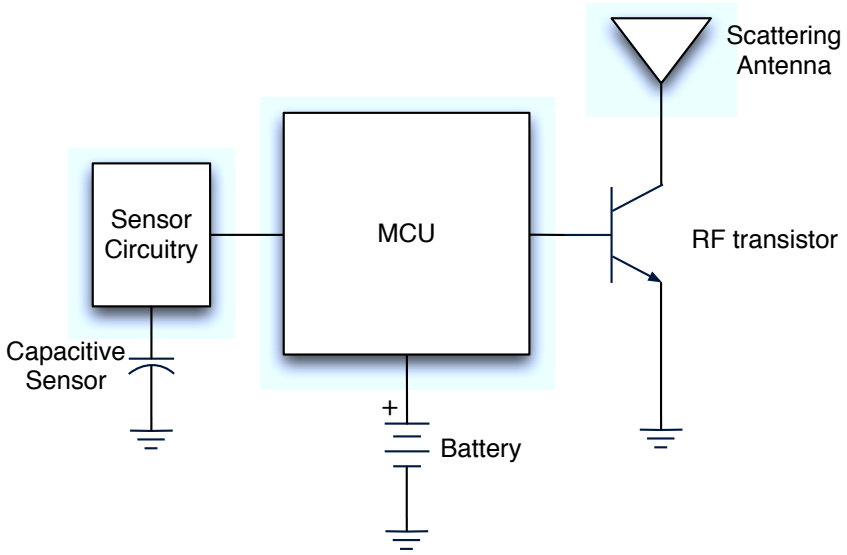

Figure 3.1: Semi-passive tag and sensor block diagram.

3.1 Hardware and PCB

When designing a WSN node, careful selection of the hardware platform needs to be made. The microcontroller unit (MCU) and radio modem used will have a great impact on the flexibility of the applications the node will be used for. Power consumption and processing capabilities highly depend on the MCU, while its architecture determines how simple the software written for it will be. A WSN node has to be as low cost as possible, thus allowing for large deployments and low replacement cost (in case of a hardware failure).

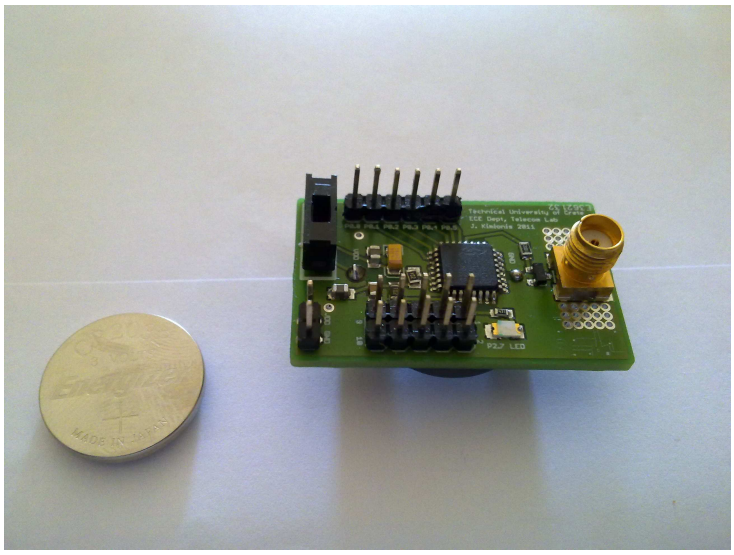

Figure 3.2: Semi-passive tag with its coin battery.

For designing a semi-passive tag, all the above have to be considered a lot more strictly compared to designing a 'classic' WSN node. The cost has to be the lowest possible, allowing for ultra-high density field deployments. This is achieved by considering two parameters. Firstly, the elimination of radio transceiver found on classic WSN nodes halves the cost, as the most expensive components are the MCU and the radio. Secondly, utilization of only the necessary components for the tag's operation without lots of paraphernalia (e.g. onboard sensors) keeps the total circuit board size small. This results to a very simple board design, which can be expanded through connectors with sensors or other external devices (e.g. data-logging memory). As for

the power consumption part, an MCU with low power operating modes has to be chosen, but without compromising the computing power or processing speeds required. A last consideration is that the tag designed should be usable in research and experimentation testbeds. This requires that software programming has to be as flexible as possible, giving access to the whole MCU instruction set, while simultaneously being relatively simple. C language programming is preferred, which fulfills both above criteria.

With the above in mind, the design employs a C8051F320 MCU from Silicon Labs. This MCU draws about $0.5mA$/MHz in normal operation and less than $0.1\mu A$ in suspend mode [14], setting it suitable for low-power applications. There are more energy-efficient MCUs, but the simple 8051 instruction set architecture (ISA) fulfills the need for simple, yet flexible software, required for scientific research. The particular MCU was incorporated in the iCube WSN node for the same reasons [3].

The tag's communication hardware consists of a UHF RF transistor and a SMA antenna connector. The transistor's gate is controlled by one of the MCU's output pins, to which it is directly connected. More on the RF part and the selection of transistors is covered in the next section.

For the MCU programming, a Silicon Labs "Debug Adapter"-compatible port is present in form of a 10-pin connector, identical to the one found on the C8051F320DK development kit [15]. For the extension of the backscatter tag's capabilities, external hardware may be connected to an I/O connector which gives access to the MCU's general purpose inputs and outputs, plus the board's power supply pins (VDD and GND). Sensor boards, like the one described in section 3.3, can be connected according to the application needs. Even actuators can be plugged into the system easily. On one of the port's output pins, an on-board general purpose LED is present, for software-controlled indications.

The MCU is powered by a 3 Volts 20mm coin battery (CR2032 type), placed in a battery holder. However, external power sources like solar panels or large capacity batteries can be plugged on the board's power supply connector.

The whole system is accommodated on a custom designed printed circuit

board (PCB). The circuit's schematic diagram was converted to PCB layout, using CadSoft's Eagle free PCB software. Routing was done manually following PCB design guidelines to decrease the impact of high frequency RF signals on digital signals lines (i.e. electromagnetic coupling) [16]. The overall board size was kept small to meet the small form factor requirement, as each node shall be easily hanged on or placed around a plant. That way, the board's manufacturing cost was also minimized. The PCB layout and circuit schematic can be found in Appendix 1.

3.2 Semi-passive tag RF part

Careful design of the RF part of a tag is crucial for efficient backscatter communication. The basic principle of modulation in backscatter radio is switching the antenna load between two values [2]. Given an antenna impedance Z_a and two impedance values Z_1 and Z_2 corresponding to the two antenna loads, two reflection coefficients Γ_1 and Γ_2 of the antenna-load system exist which are given by:

$$\Gamma_i = \frac{Z_i - Z_a^*}{Z_i + Z_a^*}, \quad i = 1, 2. \tag{3.1}$$

Each reflection coefficient corresponds to an antenna radar cross section (RCS) value given by:

$$\sigma_i = \frac{\lambda^2}{4\pi} G^2 |\Gamma_i - A_s|^2, \quad i = 1, 2, \tag{3.2}$$

where λ is the carrier wavelength, G is the antenna gain, and A_s is the (complex) antenna structural mode [10].

In the following subsections we present the design constraints for a semi-passive tag's RF part, the criteria for the selection of specific discrete RF components, and the final choice after laboratory measurements based on the theoretical constraints.

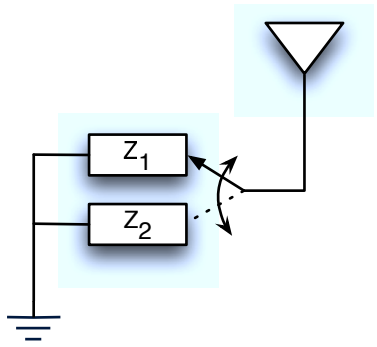

Figure 3.3: Impedance switch for backscatter modulation.

3.2.1 Design Constraints

Work in [10] has exposed the necessary conditions for efficient backscatter uplink (i.e. tag to reader) communication. The two constraints for improved tag efficiency are:

1. maximum backscattered power per bit, and
2. minimum bit error rate (BER) at the reader.

For the first constraint it is shown that maximization of average backscattered power per bit is achieved with maximization of $\{\sigma_1 + \sigma_2\}$. This is the condition for maximizing the average backscattered carrier's amplitude, on top of which information will be modulated, and thus maximization of the signal's SNR. Consequently, the possible achievable uplink range is maximized. To achieve this maximization, exact knowledge of the antenna's structural mode is required. The work in [10] provides a closed-form calculation of A_s, given the knowledge of the tag's RCS.

For the second constraint it is shown that reduced probability of detection error requires maximization of the two reflection coefficients' difference amplitude $|\Gamma_1 - \Gamma_2|$. This ensures that the two possible backscattered signals' phase or amplitude will differ as much as possible. Constellation-wise, this means the average energy per bit is maximized and so, probability of error is reduced. It is shown that for semi-passive (i.e. battery assisted) tags, where there is no need of power harvesting from the reader's carrier,

an optimal pair of reflection coefficients is $\Gamma_1 = 1$ and $\Gamma_2 = -1$. These correspond to loads $Z_1 = \infty$ and $Z_2 = 0$. The most convenient way to achieve these two load values is by using an RF transistor as a switch. Ideally, when the transistor's base is biased with a turn-on current (such that the transistor operates on the saturation region), it acts as a short circuit, and when grounded (transistor on the cutoff region) it acts as an open circuit. In a real world scenario, because of components' non-linearities, current leakages, and limited bandwidth, the two reflection coefficients will differ among components. So, among a variety of transistors, the most efficient is the one that achieves the maximum $|\Gamma_1 - \Gamma_2|$. This is the metric we use in the next subsection to characterize a series of commercially available RF transistors.

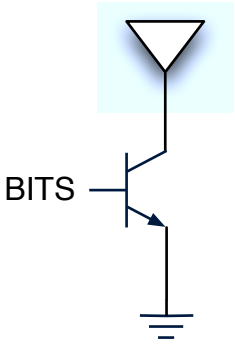

Figure 3.4: RF Transistor used as an impedance switch.

3.2.2 Transistor Measurements and Selection

To characterize a bunch of commercial discrete RF transistors, the reflection coefficients Γ_1 and Γ_2 have to be measured, for a given antenna impedance and carrier frequency. Then, their difference's absolute value can be readily calculated. We assume a UHF $\lambda/2$ dipole antenna with nominal impedance $Z_a = 50\Omega$, and carrier frequency $F_c = 867$MHz. For the measurements, a network analyzer (NA) is used, configured for single-port analysis at 50Ω, measuring the scattering parameter s_{11} of a NPN transistor's collector with common emitter, when the base is grounded, and when it is biased (Fig 3.5).

All of the RF transistors are discrete surface mount type (SMT) compo-

nents (SOT-23 footprint). Each of them is soldered, along a SMA connector for jumper cable connection with the NA and a resistor of $R = 2\text{k}\Omega$ for base biasing at $3V$, on the backscatter tag's PCB. This is done in order for the losses and/or phase changes, introduced by the PCB's traces and antenna connector, to be incorporated into the measurements. So, practically, the measured RF part is identical to the one that the final tags utilize.

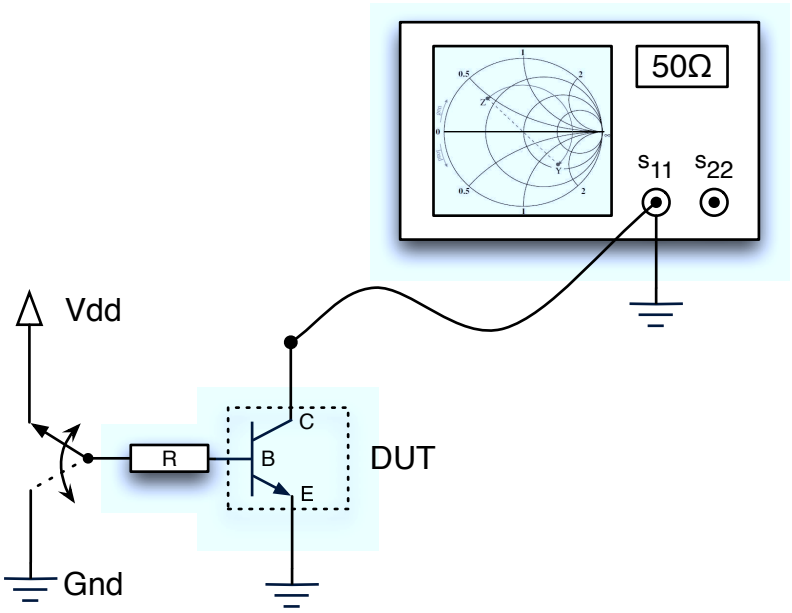

Figure 3.5: Network analyzer and transistor setup - Single port analysis.

For bigger accuracy, a 201-point reflection coefficient measurement is applied on each of the two transistor states (on/off), on a given carrier frequency. The data are exported from the network analyzer to a computer running a custom MATLAB script which averages the 201 points for each state and then calculates the absolute difference of the two (averaged) reflection coefficients). Also, a visualization of the two points, corresponding to the two transistor states, is provided on a Smith chart of impedances (e.g. Fig. 3.6).

On Table 3.2.2, the values of $|\Gamma_1 - \Gamma_2|$ for several measured transistors are shown. The one with the greater distance, and thus the most suitable among the compared transistors, is the 'NXP BFS17NTA'. It achieves

a reflection coefficient distance of 1.9991 which is very close to the optimal $|\Gamma_1^{opt} - \Gamma_2^{opt}| = |1 - (-1)| = 2$. The 'CEL NE68033-A' achieves a significantly smaller distance of 1.2084, setting it unsuitable for efficient backscatter communication, compared to the others. A visualization of this transistor's two points on the Smith chart of impedances is shown on Fig. 3.7, where the small distance between the two points can be seen clearly. Finally, the 'Agilent AT-32033' achieves a distance smaller than the 'BFS17NTA', but still close to 2, by requiring 50% less power, which could be another consideration for choosing a transistor.

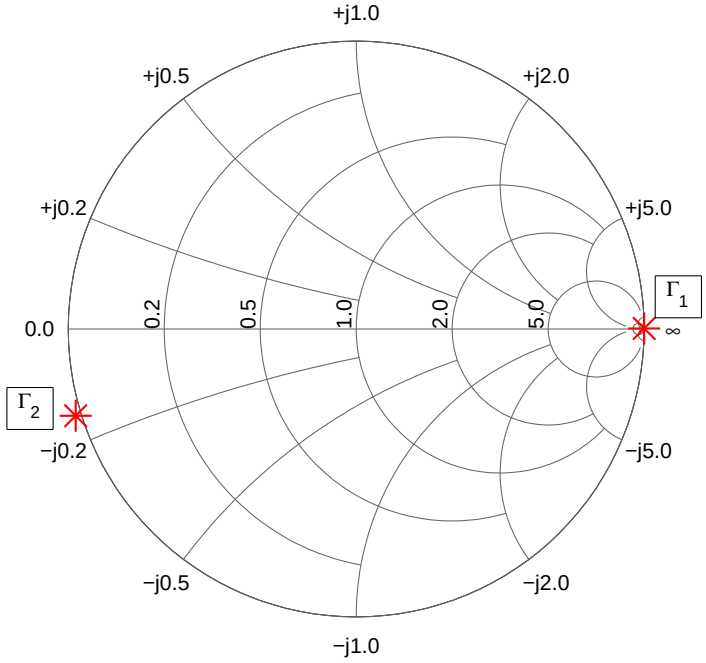

Figure 3.6: Smith chart of On/Off states for NXP BFS17NTA (normalized to 50Ω).

3.3 Sensor Circuitry

The sensor chosen for the application is the capacitive humidity sensor described in [3]. The circuit is based on a Honeywell HCH-1000 capacitor

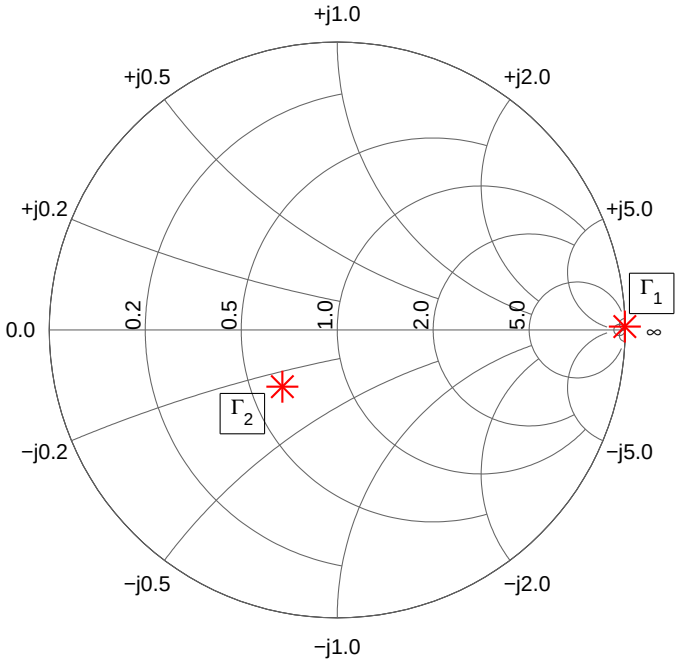

Figure 3.7: Smith chart of On/Off states for CEL NE68033-A (normalized to 50Ω).

Manufacturer	CEL	NXP	Agilent
Model	NE68033-A	BFS17NTA	AT-32033
$\|\mathbf{\Gamma_1} - \mathbf{\Gamma_2}\|$	1.2084	1.9991	1.8068
Transition Freq.	10GHz	3.2GHz	10GHz
Power Dissipation	200mW	330mW	200mW

Table 3.1: RF transistors comparison at 867MHz.

with its capacitance following a linear function of the environment's relative humidity. The capacitance value determines the frequency output of a low power 7555 timer integrated circuit. The specific circuit was chosen for its low power consumption ($\sim 300\mu A$), while not compromising its measuring range or accuracy. Additionally, its total manufacturing cost is up to four times smaller than commercially available humidity sensors, making it ideal for the low-cost backscatter network. However, its response time is higher

compared to other sensors (about 15 seconds). Nevertheless, in environmental applications humidity is not subject to quick changes, and so the sensor is of sufficient capabilities for the application's needs. Moreover, the duty cycle of measurements in such applications is usually on the order of ten minutes, which is much larger than the sensor's settling time. The software interface for this sensor detects the frequency output of the circuit by measuring the number of pulses received to the MCU in a fixed time window. Then the frequency value is translated to a relative humidity value according to the HCH-1000's datasheet.

The custom tag also utilizes an on-chip temperature sensor integrated on the C8051F320 MCU, which outputs a voltage which is proportional to the environment temperature. This is digitized by the MCU's analog to digital converter (ADC) and can be translated in the same manner the humidity sensor's output is translated.

3.4 Control Software

All tag functions, from sensing to communication are coordinated by custom software running on the 8051 MCU. Hardware peripherals of the MCU, like timers and the analog to digital converter (ADC) for temperature sensor, are also controlled by software developed in the context of this work. All software is written in simple C language.

3.4.1 Sensing

There are two sensing software interfaces, one for each type of sensor tested. The first is the frequency measurement interface, used to capture the output of the capacitive humidity sensor. Frequency pulses arrive at a general purpose input/output (GPIO) port of the tag's MCU, which is configured for external interrupt monitoring. That is, every time a 'low' ($0V$) to 'high' ($3V$) transition occurs (i.e. a pulse arrived at the GPIO), an interrupt handler is triggered and increments a pulses counter. This process is enabled only through a certain time window, in which pulses are measured. After

the end of the window, the estimated frequency is $f_{\text{est}} = \frac{\text{number of pulses}}{\text{time window in seconds}}$. Obviously, as the time window becomes longer, the estimation will be more precise. In our measurements the time window is $t_{\text{measurement}} = 1s$. The whole process is wrapped up in a function which can be called only when a measurement is desired. This means that the MCU does not always wait for interrupts, but leaves the processing core available for other tasks, like communication.

The second sensing software interface involves the use of the MCU's 10-bit analog to digital converter (ADC) for voltage measurements. The C8051F320 chip incorporates a temperature sensor which outputs a voltage value proportional to the temperature sensed. This voltage value is digitized via the ADC and can be either translated to a temperature value in software running on the node, or transmitted as raw value and translated on the reader. The ADC can also be used to measure cheap hand-made resistive humidity sensors like the ones found in [17].

3.4.2 Communication

Communication involves switching the RF transistor on or off at specific rates, depending on the modulation scheme chosen. The transistor's gate is hard-wired to the MCU's GPIO pin P0.6, which is configured as a push-pull output pin[1] and can be directly set to logic level 'high' or 'low'. The tag's modulation scheme can be set programmatically, and the transmission of a packet can be as abstract as just filling a buffer with the payload data and calling a function which takes care of the communication details.

For On Off Keying (OOK) modulation scheme and FM0 line coding (more on Section 4.4), the transistor has to remain in 'on' or 'off' state for a symbol period half of the bit duration. To keep things as precise as possible, a hardware timer that keeps track of the half-bit duration is utilized. When the timer expires, an interrupt handler is triggered, indicating that the current half-bit's transmission has ended. After that, the timer is reloaded, and the

[1]Compared to an open drain output pin, a push-pull pin can source more current to a connected load. For biasing a transistor, a high, stable current value is required.

transmission of the next half-bit begins. Bit rates for OOK are on the order of a few hundred kilobits per second.

For Frequency Shift Keying (FSK) modulation scheme, the transistor has to be switched on and off with different rates for bit '0' and bit '1', to indicate a change between the transmitted bits. Because the modulation scheme is binary-FSK, two distinct frequencies have to be generated. In contrast to OOK, where only one timer is required to keep track of the half-bit duration, for FSK an additional timer is required to generate the two frequencies. Thus, one timer keeps track of the whole bit duration, in a similar manner to the OOK (where it kept track of the half-bit duration), and the second timer, is programmed with a very short period, so as to generate a high frequency. Each time a bit changes ($0 \leftrightarrow 1$) a frequency switch is required, which can be done in two ways. With the first, the timer has to be reprogrammed at the beginning of a bit transmission to match the bit's frequency. The second, simpler approach is to run the timer with a constant high frequency (i.e. no reprogramming). For bit '1' the transistor is switched every time a timer interrupt event occurs, while for bit '0' the transistor is switched every two events. This way, the bit '0' frequency will be the half of the bit '1' frequency. This however has the downside that the distance between the two frequencies will be large, and could possibly result in a subcarrier out of the desired frequency band. With both ways of frequency generation, the frequencies must have a spacing of more than $1/T$, where T is the bit period, as required by non-coherent FSK [18].

Pseudocode examples of the communication routines can be found in Appendix 2, where MCU-specific implementation details have been left out for simplicity.

3.4.3 Alerts and Debugging

For human interaction purposes, a software-controlled LED is used for activity indication. While taking sensor measurements and transmitting data, the LED is turned on. After these tasks are complete, it is switched off for energy saving. The LED however can be programmatically switched on and

off according to the needs of the application.

Sometimes, for debugging purposes, more complex information than just a LED switching is needed. In order to output debug messages from the tag, the MCU's UART peripheral is utilized. It is used to connect the MCU via standard RS-232 serial interface to a host PC running terminal software (e.g. Minicom, HyperTerminal). After that, C-style standard input and output between the PC and the MCU are possible with ease.

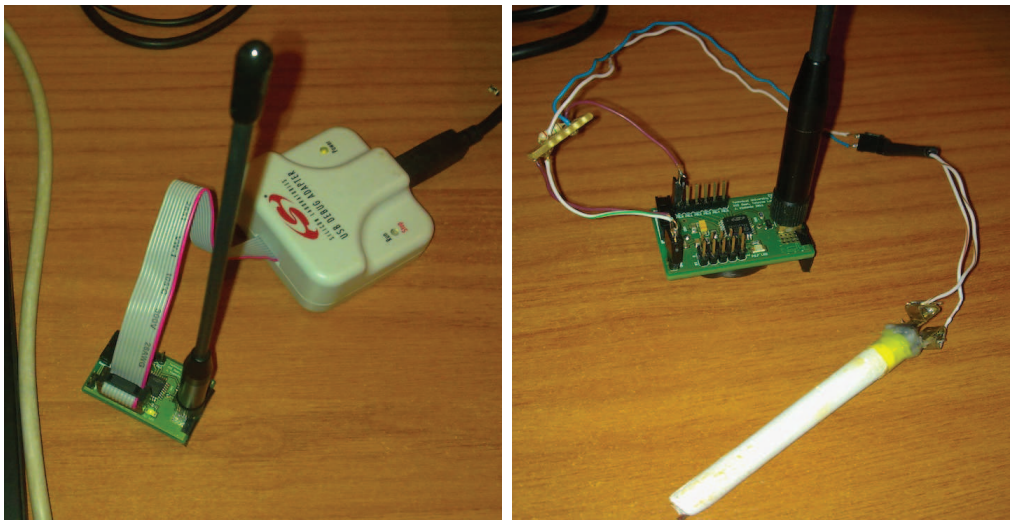

Figure 3.8: Programming a tag's MCU with the SiLabs debug adapter (left). Cheap moisture sensor made of plaster tied to a tag (right).

Chapter 4

SDR Reader Design and Backscatter Links

A backscatter link consists of a semi-passive tag, whose design was covered in Chapter 3, and a reader, which captures the tag's backscattered signals and does all the signal processing to extract the transmitted information. In this chapter, we present the reader platform, the modulation schemes used for backscatter communication, the reception of the backscattered signals, and their processing in a software defined manner.

4.1 Software Defined Reader

The whole process of reception and processing of backscattered signals is done at the *reader*. The reader consists of a receiver capable of receiving wireless transmissions on a specific frequency band, and a series of processing blocks for information extraction off the captured signals.

The reader utilized in this work is software defined, meaning it is implemented with a software defined radio platform. A software defined radio is a wireless communication system, where modulation-specific signal processing is implemented on software, leaving only the "common" procedures (i.e. downconversion, upconversion, digitizing, etc) to the hardware components. Analog signals captured off the air will be digitized and processed in a digital signal processing (DSP) manner in a PC platform. The bridge between the analog domain hardware and digital domain software are the analog to digital (ADC) and digital to analog (DAC) converters present at the SDR's hardware. This hardware/software combination makes the whole system reconfigurable, since any type of modulation/coding/processing can

be implemented in software without any change of hardware. Even several network layer protocols can be supported beyond physical layer communication protocols. Finally, the re-use of the same hardware for any communication system keeps the overall system's cost low compared to all-hardware solutions.

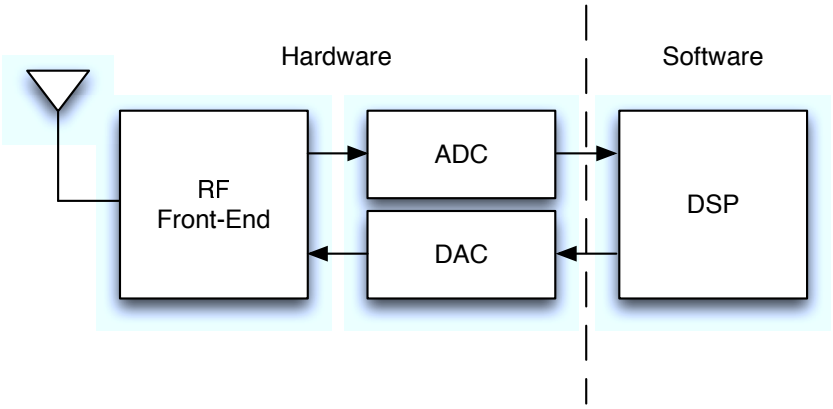

Figure 4.1: Software Defined Radio system.

4.1.1 Hardware Platform

The hardware platform used for the software defined reader is the Ettus Research Universal Software Radio Peripheral 1 (USRP1) [19]. It is an open hardware platform with freely available schematics, drivers and software base online.

The USRP consists of a motherboard which hosts 4 analog to digital converters which function as a pair of 2-channel ADCs (for in-phase and quadrature signal digitizing) and 4 digital to analog converters which similarly function as a pair of 2-channel DACs. Also, a field programmable gate array (FPGA) chip is present on the board for digital down- and up-conversion, and other high rate signal processing. Finally, it utilizes a USB interface for PC connectivity.

Up to 2 transceiver daughterboards can be plugged onto the USRP's motherboard. A daughterboard hosts the analog RF front-end for wireless

reception and transmission. All mixing, filtering, and amplification is done on the daughterboard. Ettus ships a family of daughterboards for all spectrum bands from DC up to 6 GHz; in order to change the desired operating band, one has to use the corresponding daughterboard, leaving the USRP motherboard untouched. This makes the system even more cost-effective.

The reader's analog front-end is a RFX900 daughterboard, capable of capturing signals on the UHF band (800 MHz - 1.0 GHz). The motherboard is a USRP1 with 64 Msamples/sec ADCs, capable of digitizing up to 16 MHz bandwidth of In-phase/Quadrature signals. Due to the limitations of the USB interface, though, only up to 8 MHz can be 'seen' by the PC host. There is also a software-controllable decimation filter running on the board's FPGA that acts as a low-pass filter for decreasing the sampling rate by a factor of 1 to 256. That is, the total bandwidth seen by the PC can be anything from 31.25 kHz to 8 MHz.

4.1.2 Software Platform

The software platform of reader consists of two main parts. The first one is GNU Radio, the open source software counterpart for the USRP, which consists of a library of signal processing blocks written in C++ and a Python interface for interconnecting blocks. Complete communication systems can be built from the GNU Radio blocks which cover many functions; from USRP transmit and receive interfaces to demodulation blocks and graphical sinks (FFT plots, oscilloscopes, etc.). However, throughout this work, GNU Radio is only used as the software interface for bringing digitized samples from the USRP to the PC.

The second part of the software platform is the MATLAB environment. Although some functions for the processing required by the reader can be found readily available in GNU Radio blocks, these are implemented in custom MATLAB code for greater control over the system's DSP. Note that some of these functions can also be found in MATLAB's Simulink environment under the "Communications Toolbox" and other ready-provided blocksets, but as already explained, all the DSP is built from scratch with custom code.

Both pieces of software run on a Linux environment, but other platforms (Mac OS X or Windows) could be also used. Intercommunication between the GNU Radio interface and MATLAB is done using standard UNIX pipes (FIFOs) (on Windows, due to the lack of pipes, third party tools can be used to bring USRP data in MATLAB, like [20]). So the complete receive chain consists of a USRP capturing and downconverting signals, then passing the digitized signals to GNURadio by USB. The samples are brought through a FIFO to MATLAB, where they are processed. A block diagram is shown in Fig. 4.2.

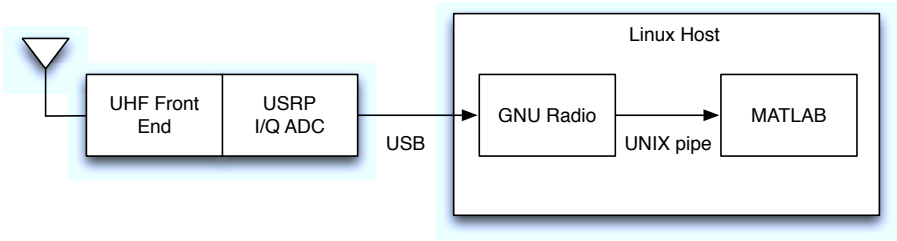

Figure 4.2: Software defined reader receive chain.

4.2 Signal Model

We assume the simple channel model of Fig. 4.3. The signal generator transmits a constant wave with amplitude A which arrives at the software defined reader scaled by a factor B and rotated by a phase $\Delta\phi$. The carrier also arrives at the tag scaled by C and rotated by c, which is modulated by the baseband signal $Sx(t)$; S is a simple term which depends on the tag's backscattering efficiency.[1] The modulated signal is backscattered and arrives at the reader scaled by D and rotated by d. The noiseless received signal at

[1]Complete formulation of the backscattered signal's amplitude, with reference to the tag's radar cross section values can be found in [10].

the reader is

$$\begin{aligned} y_{\text{nl}}(t) &= [ABe^{-j\Delta\phi} + ACe^{-jc}SDe^{-jd}x(t)]\ e^{-j2\pi\Delta Ft} \\ &= Ae^{-j2\pi\Delta Ft - j\Delta\phi}[B + CSDe^{-j\phi_0}x(t)], \end{aligned} \tag{4.1}$$

where ΔF is the carrier frequency offset (CFO) between the signal generator and the reader, and $\phi_0 = c + d - \Delta\phi$. A, B, C and D are positive quantities. The noisy received signal is

$$y(t) = y_{\text{nl}}(t) + n(t), \qquad n(t) \sim \mathcal{CN}(0, \sigma_n^2). \tag{4.2}$$

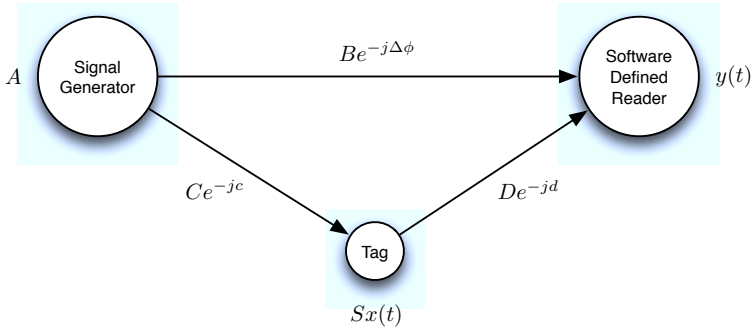

Figure 4.3: Backscatter channel model.

In the simple case of additive white gaussian noise (AWGN) channels (that is $Be^{-j\phi_0} = Ce^{-jc} = De^{-jd} = 1$) and no CFO the received signal would be

$$y_{\text{AWGN}}(t) = A\ [1 + S\ x(t)] + n(t), \qquad n(t) \sim \mathcal{CN}(0, \sigma_n^2). \tag{4.3}$$

The physical explanation for the above equation is that the tag's waveform, with a small amplitude, stems on top of a high amplitude DC, as shown in Fig. 4.4.

The DC's amplitude depends on the signal generator's output power and the higher it is, the longer the range will be, as the total signal's power $P_T = \mathcal{E}\{|y_{\text{nl}}(t)|^2\}$ grows proportionally to the square of A. From Friis transmission equation it holds that the power of a received signal at distance d from the

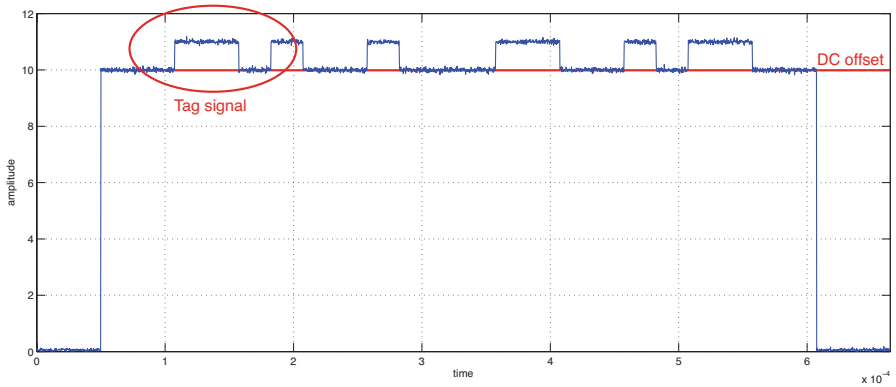

Figure 4.4: Magnitude of the In-phase and Quadrature components at the reader ($\sqrt{I^2(t) + Q^2(t)}$).

transmitter is proportional to the transmitted power

$$P_R = G_T G_R \left(\frac{\lambda}{4\pi d}\right)^2 P_T, \tag{4.4}$$

where G_T, G_R are the transmit and receive antenna gains respectively, and λ is the carrier wavelength. So the higher the carrier's power is, the greater the range that can be covered for a given receiver sensitivity and tag backscatter efficiency. Also, note that the tag waveform's amplitude grows proportionally to A, which means that the signal-to-noise-ratio (SNR) for a tag reply grows when the carrier power grows. In Fig. 4.5, the same tag transmission is shown for two different carrier power values. The generator, the tag and the reader are in fixed places and thus channel attenuation is the same for both cases. The waveforms are normalized to the highest received amplitude level. Notice that by lowering the generator's transmit power by 6dB, the DC corresponding to the carrier is halved. Notice also that the distance between the two backscattered levels is halved, i.e. the signal's SNR is lowered by 6dB. This is used extensively throughout the experiments of this work to adjust the tag signal's SNR by controlling the generator's output power.

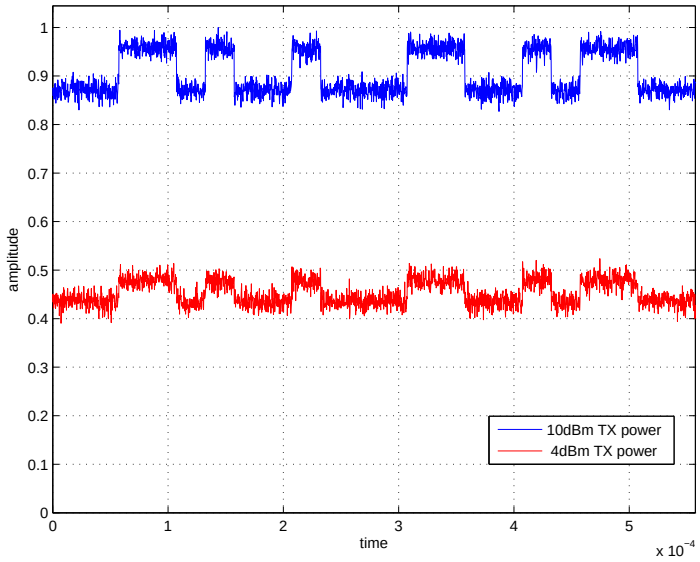

Figure 4.5: Received signals for different carrier power levels.

4.3 Digital Signal Processing for Received Backscatter Signals

After the reception and downconversion from the analog RF front end, the baseband signal, sampled by the ADCs arrives in the form of digital samples at the PC. In this section we present the digital signal processing (DSP) chain for received signals in MATLAB environment.

4.3.1 I/Q Samples

In-phase and quadrature samples from the ADCs arrive in an interleaved form at the buffer to be read by MATLAB. That is, I and Q samples are stored alternately in the buffer, as shown in Fig. 4.6. For convenience in processing, the series of I and Q samples is converted to a series of complex values, resulting in a complex baseband signal. This process is called deinterleaving. For each pair of I/Q samples, the quadrature component is multiplied by the imaginary unit j and summed with the in-phase component, resulting in a

complex value.

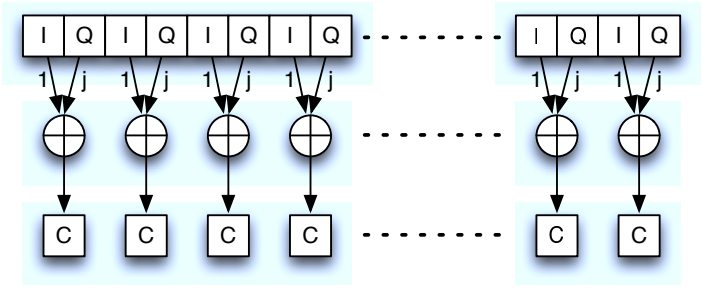

Figure 4.6: Deinterleaving of I/Q samples and conversion to complex samples.

4.3.2 Magnitude of Complex Baseband Signal

In the case of a bistatic reader architecture, the carrier signal generator and the receiving software defined radio are two different boxes, each utilizing its own oscillator for up- and down-conversion, respectively. This results in a frequency and phase offset between the two, due to the variable tolerance of the oscillators and their fluctuations due to the changes of environment temperature. In signal model of Eq. 4.1, the carrier frequency offset ΔF has been taken into account, and the carrier phase offset can be considered to be a part of the phase $\Delta\phi$ introduced by the channel B.

By taking the magnitude of the complex signal $y_{\text{nl}}(t)$ we have

$$y_{\text{mag}}(t) \triangleq |y_{\text{nl}}(t)| = A|B + CSDe^{-j\phi_0}x(t)| \tag{4.5}$$

This way, the carrier frequency and phase offsets are eliminated. However, an unknown phase ϕ_0 that rotates the tag signal is still present. Note that, for noisy inputs, with complex Gaussian distribution, the observed signal's magnitude does not follow a Gaussian distribution. This is explained in section 4.3.2. In the case of a monostatic reader, the carrier transmitted and the carrier used for demodulation come from the same oscillator, so no frequency offset is present [2]. However, an unknown carrier phase offset may

still be present, which results in a scaling of the received signal on the in-phase and quadrature branches of the receiver. Since non-coherent detection is the common case in backscatter, either one or both of the in-phase or quadrature branches can be processed, according to e.g. the signal strength in each branch. Maximum ratio combining (MRC) of the two branches requires estimation of the phase offset, which is not an option in low-bitrate backscatter, because of the quick changing nature of the wireless channel.

Noise

Because of the complex baseband signal's magnitude extraction, which is a non-linear process, the observed signal changes characteristics and is no longer Gaussian which could affect maximum likelihood (ML) detection of the tag's transmitted symbols. However, under certain circumstances, the observed signal's probability density function (PDF) can be well approximated by a Gaussian PDF.

Someone could mistakenly assume that because the noise in a backscatter link is complex gaussian ($n \sim \mathcal{CN}(0, \sigma_n^2)$) and the noise's magnitude follows the Rayleigh distribution

$$f_{|n|}(n) = \frac{2n}{\sigma_n^2} e^{-\frac{n^2}{\sigma_n^2}}, \quad n \geq 0, \tag{4.6}$$

that the received signal's magnitude M will also follow the Rayleigh distribution. This is wrong, as for a received DC a, in general it holds that

$$M = |a + n| \neq a + |n| \Rightarrow f_M(M) \neq a + f_{|n|}(n), \tag{4.7}$$

where $f_M(M)$ is the DC and noise sum's amplitude probability density function, and $f_{|n|}(n)$ is the complex gaussian noise's amplitude probability density function (which is Rayleigh). The received signal's magnitude would follow a Rayleigh distribution, if only zero-mean complex gaussian noise was present at the received signal (i.e. $a = 0$). However, the probability density function of the received signal's magnitude depends both on the complex normal noise and the noiseless received signal.

Assuming transmission of a carrier wave from the signal generator and reception of it at the reader with amplitude a, the baseband received signal, ignoring carrier frequency and phase offsets, will be

$$\begin{aligned} y(t) &= a + n(t), \quad n(t) \sim \mathcal{CN}(0, \sigma_n^2) \\ &= a + n_I(t) + jn_Q(t), \quad n_I(t), n_Q(t) \sim \mathcal{N}(0, \frac{\sigma_n^2}{2}). \end{aligned} \tag{4.8}$$

The magnitude

$$M = \sqrt{(a + n_I(t))^2 + n_Q^2(t)} \tag{4.9}$$

of such a signal follows the Rice distribution [21], [22]

$$f_M(M|a) = \frac{2M}{\sigma_n^2} e^{-\frac{M^2+a^2}{\sigma_n^2}} I_0(\frac{2aM}{\sigma_n^2}), \quad M \geq 0, \tag{4.10}$$

where I_0 is the zeroth order modified Bessel function of the first kind. We expand Eq. 4.9 to a more general form to use for a received baseband signal assuming carrier frequency and phase offset.

***Lemma* 1.** *$\sqrt{z_1'^2 + z_2'^2}$, with $z_1' \sim \mathcal{N}(a\cos\phi, \frac{\sigma_n^2}{2})$ and $z_2' \sim \mathcal{N}(a\sin\phi, \frac{\sigma_n^2}{2})$, follows a Rice distribution.*

Proof. In general, when A is a real number and $n_1, n_2 \sim \mathcal{N}(0, \frac{\sigma_n^2}{2})$, the quantity $M = \sqrt{(a + n_1)^2 + n_2^2}$ follows a Rice distribution. We assume that M is the magnitude of the complex number

$$\begin{aligned} z &= z_1 + jz_2 = (a + n_1) + jn_2 \\ &= a + n, \quad n = n_1 + jn_2 \sim \mathcal{CN}(0, \sigma_n^2). \end{aligned} \tag{4.11}$$

Then we have

$$\begin{aligned}
M &= |z| = |z|\ 1 = |z||e^{j\phi}| = |ze^{j\phi}|, \qquad \phi \in [0, 2\pi) \\
&= |(a+n)e^{j\phi}| = |ae^{j\phi} + \underbrace{ne^{j\phi}}_{n' \sim \mathcal{CN}(0,\sigma_n^2)}| \\
&= |ae^{j\phi} + \underbrace{n'}_{n'=n'_1+jn'_2}| = |a\cos\phi + ja\sin\phi + n'_1 + jn'_2| \\
&= |(a\cos\phi + n'_1) + j(a\sin\phi + n'_2)| = |z'_1 + jz'_2| \\
&= \sqrt{z'^2_1 + z'^2_2}, \quad \text{with } z'_1 \sim \mathcal{N}(a\cos\phi, \frac{\sigma_n^2}{2}), z'_2 \sim \mathcal{N}(a\sin\phi, \frac{\sigma_n^2}{2}). \qquad (4.12)
\end{aligned}$$

□

Again, reminding the assumption of a single carrier transmission and reception of amplitude a with carrier frequency and phase offsets being present, the baseband received signal is

$$\begin{aligned}
y(t) &= a\ e^{-j2\pi\Delta Ft - j\Delta\phi} + n(t), \quad n(t) \sim \mathcal{CN}(0, \sigma_n^2) \\
&= a\ e^{-jv(t)} + n(t), \qquad (4.13)
\end{aligned}$$

where $v(t) = 2\pi\Delta Ft + \Delta\phi$. This can be written through Euler's formula as

$$\begin{aligned}
y(t) &= A\cos v(t) - jA\sin v(t) + n(t) \\
&= y_I(t) - jy_Q(t), \qquad (4.14)
\end{aligned}$$

where $y_I(t), y_Q(t)$ are the in-phase and quadrature received components, respectively, which are:

$$y_I(t) = a\cos v(t) + n_I(t), \quad n_I(t) \sim \mathcal{N}(0, \frac{\sigma_n^2}{2}), \qquad (4.15)$$

$$y_Q(t) = a\sin v(t) + n_Q(t), \quad n_Q(t) \sim \mathcal{N}(0, \frac{\sigma_n^2}{2}). \qquad (4.16)$$

After the magnitude extraction of $y(t)$, we have

$$y_{\text{mag}}(t) = |y(t)| = \sqrt{y_I^2(t) + y_Q^2(t)}. \qquad (4.17)$$

Since it holds that $y_I(t) \sim \mathcal{CN}(a\cos v(t), \frac{\sigma_n^2}{2})$ and $y_Q(t) \sim \mathcal{CN}(a\sin v(t), \frac{\sigma_n^2}{2})$, from *Lemma 1*, $y_{\text{mag}}(t)$ follows a Rice distribution.

It is stated in the literature that the Rice distribution can be approximated well by a Gaussian distribution for values of $\frac{a}{\sigma_n/\sqrt{2}} > 3$, and coincides with the Rayleigh distribution when $a = 0$ [23]. In a backscatter radio link, the first is the common case, as the received carrier a is usually more intense than the additive noise ($a^2 >> \sigma_n^2$), while noise power is still comparable to the tag signal's power.

Thus, the received signal's magnitude is a sufficient statistic for tag decoding which follows the Rice distribution. For high carrier-to-noise ratio values the observed magnitude's PDF is approximated by a Gaussian distribution, and so, ML detection is expected to show similar detection performance with the already-known ML detection in AWGN channels, for which BER closed-forms are readily available in the literature.

4.3.3 Matched Filtering / Symbol Correlators

The received signal is subject to noise, which affects detection dramatically if its power is comparable to the useful signal's power. It is known that by using a pulse matched filter to filter the signal, the signal to noise ratio (SNR) is maximized at the center of the symbol, which is the optimal sampling position [18]. Given a transmit pulse $g_T(t)$, its matched counterpart is $g_R(-t)$ (i.e. the reflection of the transmit shaping pulse). For a received signal y, the pulse matched filtered waveform is

$$y_{\text{low}}(t) = y_{\text{mag}}(t) * g_R(t) = y_{\text{mag}}(t) * g_T(-t), \tag{4.18}$$

where $*$ is the linear convolution operator.

For non-coherent binary FSK modulation, two quadrature correlators are used at the receiver to correlate the incoming signal with the mark/space frequencies [18]. Given a basis function $g_T(t)$ for a symbol, the in-phase and

quadrature branches of the correlator will be

$$g_R^{(I)}(t) = g_T(-t) \tag{4.19}$$

$$g_R^{(Q)}(t) = \tilde{g}_T(-t), \tag{4.20}$$

where $\tilde{g}_T$ is the $\pi/2$ shifted-phase counterpart of g_T (i.e. for $g_T = \cos(\cdot)$, it is $\tilde{g}_T = -\sin(\cdot)$). Note that this also means filtering the observed signal $y_{\text{mag}}(t)$ around the correlated frequencies (bandpass filtering).

4.3.4 Envelope Extraction

For binary modulations, common in backscatter systems, decision on the received bits is based on the comparison of the matched filters outputs' envelopes. For baseband matched filters (e.g. in the case of amplitude modulation) this is not necessary, because information is already there; on the amplitude of the matched filter's output. However, in the case of non-coherent FSK modulation, the outputs of the in-phase and quadrature branches of each frequency correlator have to be combined to get the amplitude of the output. The amplitude is taken by squaring the outputs of the in-phase and quadrature branches and summing them, then calculating the square root of the result.

For binary FSK where two correlators (mark/space frequencies) are used to correlate the incoming signal, we extract two envelopes $\hat{y}_{\text{low},0}(t)$ and $\hat{y}_{\text{low},1}(t)$, and then form the total envelope

$$r(t) = \hat{y}_{\text{low},1}(t) - \hat{y}_{\text{low},0}(t). \tag{4.21}$$

4.3.5 Packetizing - Coarse Time Synchronization

Packetizing is a crucial process for a packet-based communication scheme, where a data buffer is split into smaller segments that (most likely) contain a full packet of transmitted data. In our software defined reader two packetizing methods are implemented. The first one is an energy-based packetizer, which calculates the total signal power in a sliding time window, and com-

pares the power ratio between two consecutive windows. If the power ratio exceeds a threshold, a packet's start is expected to be present [24]. The second is a preamble correlation packetizer, which uses a sliding correlator to detect the packet's preamble symbols in the total formed envelope $r(t)$. The maximum of the correlation occurs at the point where the first symbol is [25].

Because many packets may be present in a buffer, both processes will result in a peak at each packet's beginning. After each packet's coarse start has been detected, the packet's data with a number of samples before the beginning and after the end are placed in a smaller buffer for further processing. The packetizer has to verify the integrity of a packet to be processed according to its length, i.e. if the packet is 'split' at the end of the buffer, its length will be shorter than the one expected. In a simple scenario this packet could be discarded from processing, or in a more sophisticated packetizing scheme, the first half of the packet in a buffer could be stored to unify with its second half, when a new buffer is available for processing.

4.3.6 Fine Symbol Synchronization

After the packetizing process, the exact position of the packet's first symbol has to be found. Assuming that the first sampling position is at time instant $t = \tau$, which is unknown, an estimation of τ is needed for correct sampling timing. A preamble correlator is used to find the first sampling position in the manner that the correlation packetizer does. Actually, fine symbol synchronization is not necessarily needed if a correlation packetizer was used, but is indeed necessary after coarse packet synchronization using the two windows' energy method.

4.3.7 Sampling

After the symbol synchronization process, a first sampling position τ has been found. By sampling at the time instants $t = nT + \tau, n = 0, \ldots N-1$,

we get the discrete-time sequence

$$r_n = r[n] = r(nT + \tau) \tag{4.22}$$

which are the samples at the optimum (SNR-wise) positions that correspond to the bits transmitted [18], [24].

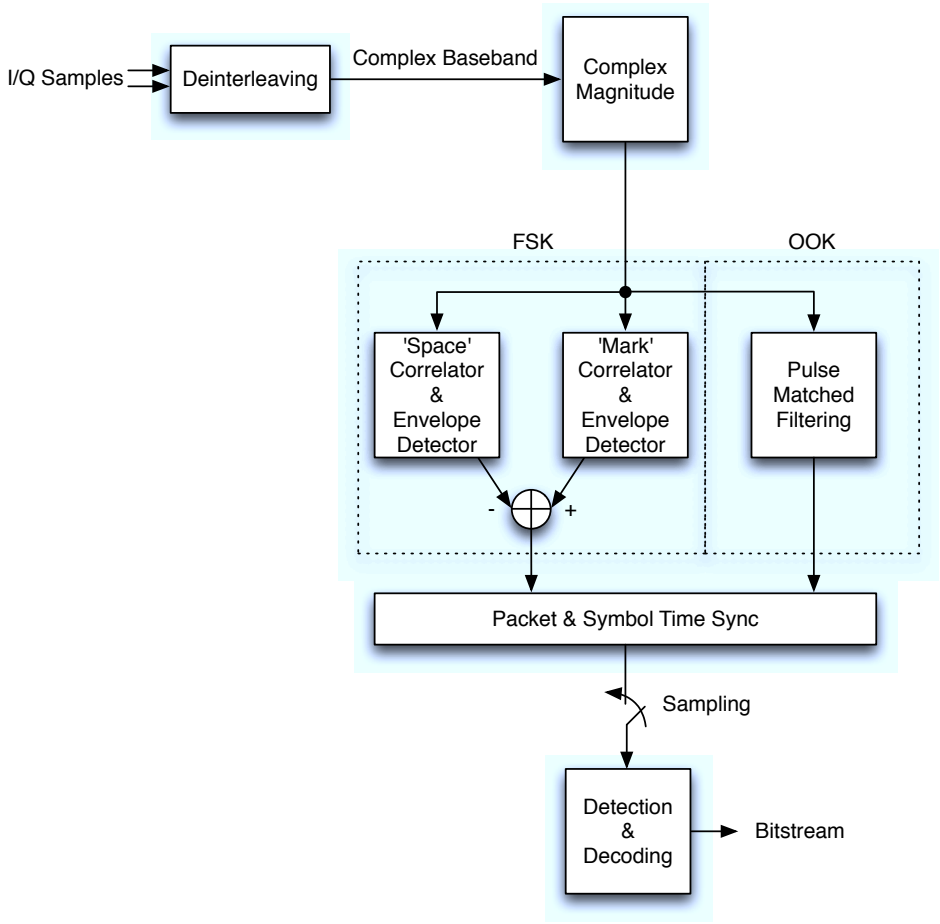

Figure 4.7: Digital Signal Processing chain.

4.4 Modulation Schemes

In this section we are going to show two modulation schemes used for backscatter communication. The first one is the simplest form of non-coherent am-

plitude modulation, called On-Off Keying (OOK). Bits "1" and "0" are represented by a high power level, or no power level, respectively. The second one, is a form of non-coherent Frequency Shift Keying (FSK). Bit "1" and "0" are represented by changes in frequency of a backscattered pulse-train.

In both modulation schemes, the RF Signal Generator transmits a sinusoid of the form $c_{\mathrm{PB}} = 2A\cos(2\pi F_c t)$ with a baseband equivalent $c_{BB}(t) = A$. For simplicity, the two transistor states of a tag will correspond to the two levels '0' and '1'. Thus, any tag waveform is considered to switch between $\{0, 1\}$.

4.4.1 OOK Modulation Scheme

Since the tag can only switch the transistor on or off and thus, cannot perform any pulse shaping (e.g. raised cosine filter, gaussian filter), its baseband pulses are of the form

$$g_T(t) = \begin{cases} 1, & -T/2 \leq t < T/2, \\ 0, & \text{elsewhere}, \end{cases} \tag{4.23}$$

where T is the symbol period.

Assuming the transmitted bits $a_n = \{0, 1\}, n = 0, \ldots N-1$, the baseband tag waveform is of the form

$$x(t) = \sum_{n=0}^{N-1} a_n \; g_T(t - nT) \tag{4.24}$$

After pulse-matched filtering, time synchronization and sampling at time instants $t = nT + \tau, n = 0, \ldots N-1$, we retrieve the sequence

$$r_n = r[n] = r(nT), \tag{4.25}$$

which in absence of additive noise will be of two distinct levels:

$$r_n = \begin{cases} A|B + CSDe^{-j\phi_0}|, & \text{if } a_n = 1 \\ AB, & \text{if } a_n = 0. \end{cases} \tag{4.26}$$

These are sufficient statistics for estimation of a_n. Maximum likelihood (ML) decision on the transmitted bits is based on the rule

$$a_n^{\text{est}} = \begin{cases} 1, & \text{iff } r_n > \frac{AB + A|B + CSDe^{-j\phi_0}|}{2} \\ 0, & \text{else,} \end{cases} \tag{4.27}$$

which is a minimum distance detector (MDD). MDD is a ML detector, as long as the sufficient statistics follow a Gaussian distribution. This is the case under certain conditions, as it was shown in subsection 4.3.2. To follow this decision rule, knowledge of A, B, C, S, D and ϕ_0 is required for threshold calculation (i.e. coherent detection). However, the threshold value can be estimated roughly as the mean value of r_n of long training symbol sequences where the two possible bit values are equiprobable. Note that a symbol reverse may have happened due to the exponential in Eq. 4.26, i.e. low level may correspond to bit '1' instead of bit '0'. This can be also estimated by the training sequence. Adaptive methods for threshold calculation in non-coherent OOK could be also applied (e.g. [26]), but they have not been examined in the context of this work.

FM0 Line Code

In Generation 2 UHF RFID standard, the default *uplink* signaling (tag to reader) is FM0 coding in amplitude modulation schemes [13]. A flip of the transistor's state is required at each bit boundary, even if two consequent bits are the same. A bit '0' waveform has an additional transition in the middle of the bit duration, while bit '1' waveform retains its line level for the whole bit duration.[2] This way, the bit is decoded based on the duration

[2]FM0 is also known as *biphase space* because of the transition in the middle of the space ('0') bit.

of each pulse, and not on its level, which is useful if the tag signal arrives at the reader in such a way that its phase is inverted. FM0 line code has a single-bit memory which can be exposed for efficient detection, as shown in [27]. Exploiting the FM0's memory characteristics can improve bit detection performance in terms of BER by 3dB.

In Fig. 4.9, a pulse-matched filtered baseband OOK waveform is shown, along with the corresponding *raw* received I/Q components (CFO-present), and their FFT. In Fig. 4.10, the spectrum of a backscatter OOK transmission observed with a spectrum analyzer can be seen.

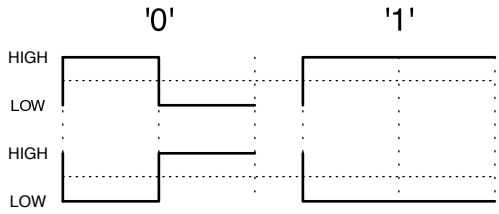

Figure 4.8: FM0 bit waveforms.

4.4.2 FSK Modulation Scheme

The two basis functions used to modulate data using binary frequency shift keying (2-FSK) are

$$g_{T,0}(t) = \cos(2\pi F_0 t), \qquad -T/2 \leq t < T/2 \tag{4.28}$$

$$g_{T,1}(t) = \cos(2\pi F_1 t), \qquad -T/2 \leq t < T/2, \tag{4.29}$$

where F_0 and F_1 are the space and mark frequencies, respectively. Frequencies are chosen so that $F_1 > F_0 + 1/T$, to ensure orthogonality between the two basis functions in non-coherent FSK [18]. We use the following notation for the basis functions

$$g_T(i,t) = g_{T,i}(t) = \cos(2\pi F_i t), \qquad i = 0, 1. \tag{4.30}$$

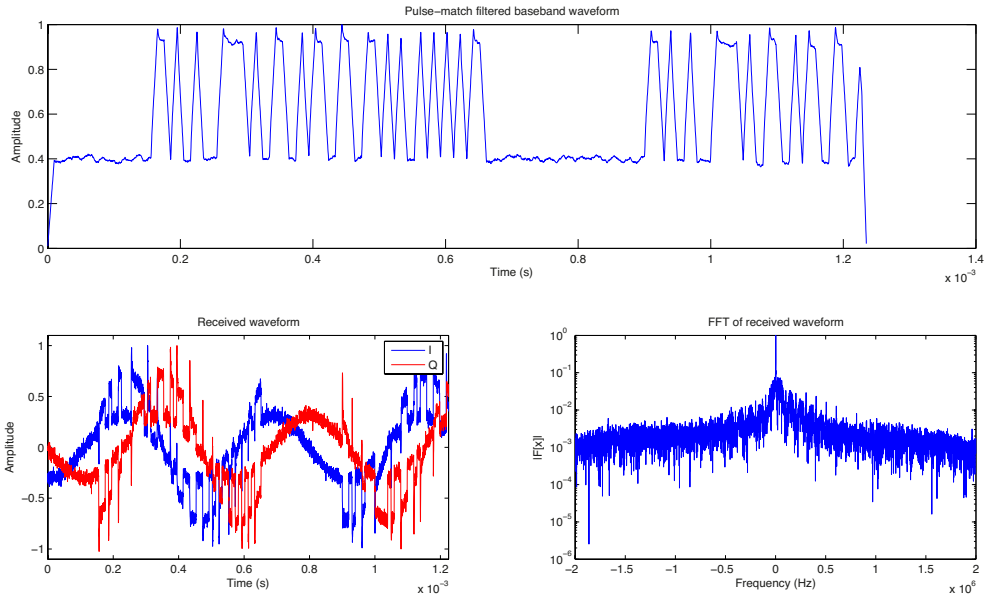

Figure 4.9: OOK baseband filtered waveform (top), the raw received components (bottom-left), and their FFT (bottom-right).

Because the tag can only switch the RF transistor on or off, the basis functions become

$$(\mathrm{sgn}\{g_T(i,t)\}+1)/2, \qquad i=0,1, \qquad -T/2 \le t < T/2 \tag{4.31}$$

where $\mathrm{sgn}(\cdot)$ is the signum function

$$\mathrm{sgn}(k) = \begin{cases} -1, & \text{if } k<0, \\ 0, & \text{if } k=0, \\ 1, & \text{if } k>0. \end{cases} \tag{4.32}$$

The baseband tag waveform is of the form

$$x(t) = \frac{1}{2} + \frac{1}{2}\sum_n \mathrm{sgn}\{g_T(a_n, t-nT)\} \tag{4.33}$$

Such a waveform is shown in Fig. 4.11.

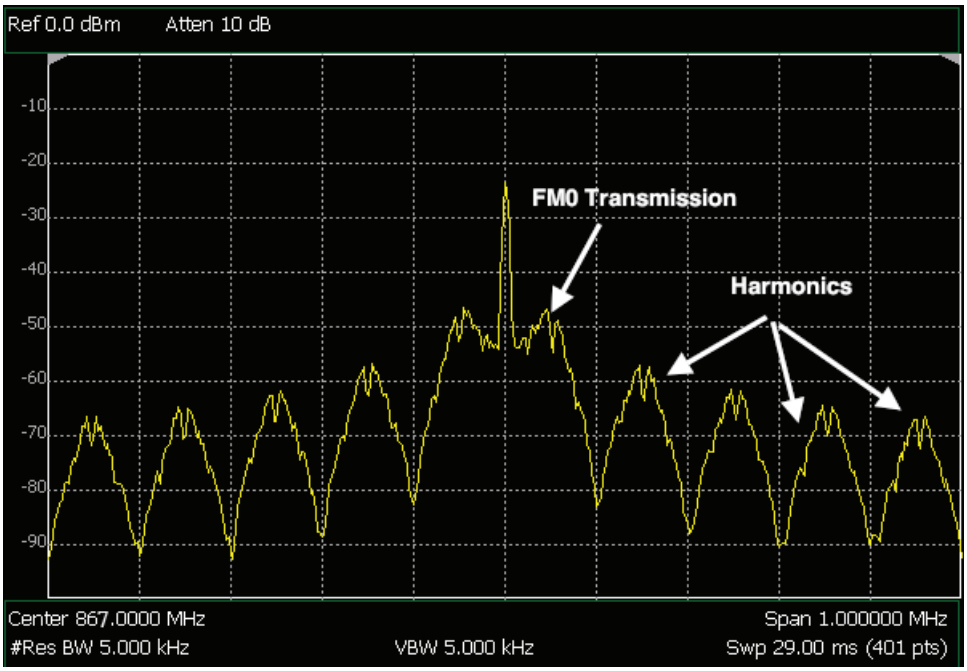

Figure 4.10: OOK backscatter transmission observed with a spectrum analyzer.

Two correlators, $\{g_{R,0}^{(I)}(t), g_{R,0}^{(Q)}(t)\}$ and $\{g_{R,1}^{(I)}(t), g_{R,1}^{(Q)}(t)\}$, are used to correlate the incoming signal with the space and mark frequencies, respectively. The envelopes of the correlators' outputs are:

$$\hat{y}_{\text{low},0}(t) = \sqrt{[y_{\text{mag}}(t) * g_{R,0}^{(I)}(t)]^2 + [y_{\text{mag}}(t) * g_{R,0}^{(Q)}(t)]^2}, \tag{4.34}$$

$$\hat{y}_{\text{low},1}(t) = \sqrt{[y_{\text{mag}}(t) * g_{R,1}^{(I)}(t)]^2 + [y_{\text{mag}}(t) * g_{R,1}^{(Q)}(t)]^2}. \tag{4.35}$$

The total envelope is formed

$$r(t) = \hat{y}_{\text{low},1}(t) - \hat{y}_{\text{low},0}(t). \tag{4.36}$$

After sampling the total envelope of the correlators at time instants $t = nT, n = 0, \ldots N-1$, we retrieve the sequence

$$r_n = r[n] = r(nT). \tag{4.37}$$

Decision on the transmitted bits is based on the rule

$$a_n^{\text{est}} = \begin{cases} 1, & \text{iff } r_n > 0 \\ 0, & \text{else.} \end{cases} \tag{4.38}$$

In Fig. 4.12, the frequency domain of a backscatter FSK transmission observed with a spectrum analyzer is shown. Two subcarriers corresponding to the space/mark frequencies, along with their odd harmonics (due to 50% duty-cycle rectangular pulses from transistor switching operation) can be seen.

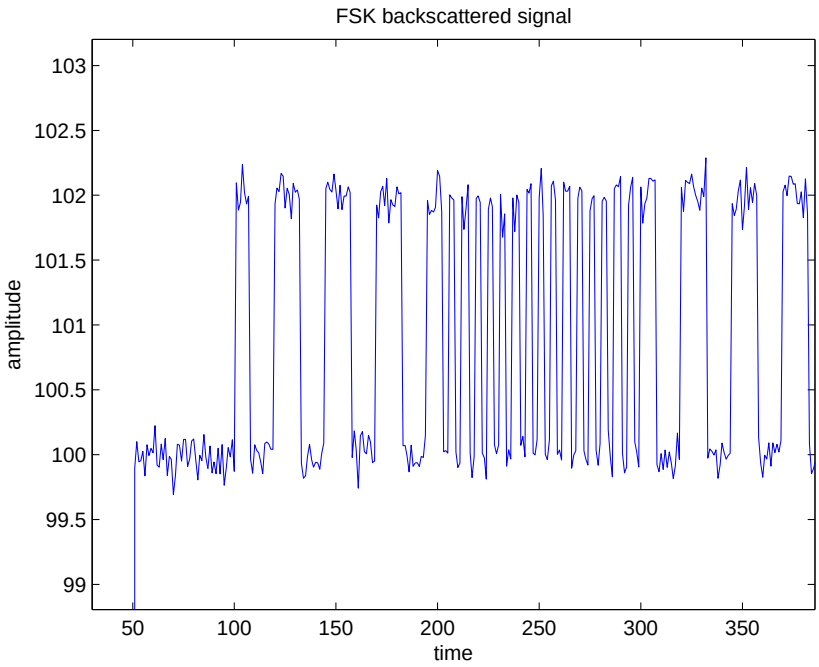

Figure 4.11: FSK backscatter baseband waveform.

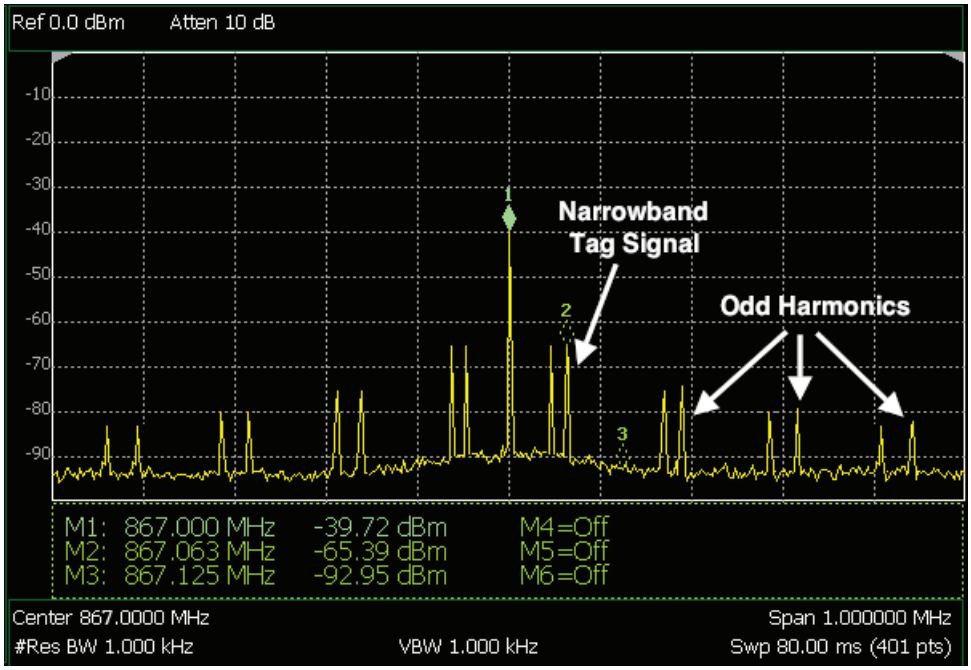

Figure 4.12: FSK backscatter transmission observed with a spectrum analyzer.

4.5 BER Performance

4.5.1 OOK

Probability of detection error for On Off Keying can be calculated easily. Being a binary modulation, the BER is of the form $Q\left(\frac{d}{2\sigma}\right)$, where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{+\infty} e^{-t^2/2}dt$ is the Q function, d is the distance of the two constellation points, and σ is the (Gaussian) noise deviation at the output of the matched filter, sampled at the correct time instance [18]. For OOK with constellation points 0 and b, $d = b - 0 = b$. The (average) bit energy is $\mathcal{E}_b \propto \frac{0^2+b^2}{2} = \frac{b^2}{2}$, so $b \propto \sqrt{2\mathcal{E}_b}$. The noise deviation is $\sigma \propto \sqrt{N_0/2}$. We have

$$P_b^{\text{OOK}} = Q\left(\frac{b}{2\sigma}\right) = Q\left(\frac{\sqrt{2\mathcal{E}_b}}{2\sqrt{N_0/2}}\right) = Q\left(\sqrt{\frac{\mathcal{E}_b}{N_0}}\right), \tag{4.39}$$

with $\mathcal{E}_b = \frac{b^2}{2}T$.

Analysis considers perfect knowledge of the optimum threshold for bit

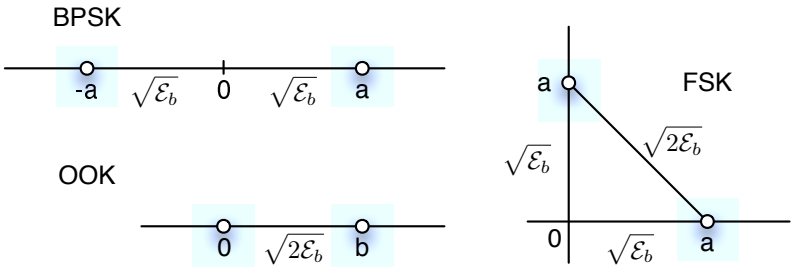

Figure 4.13: OOK and FSK constellations compared to the BPSK constellation.

discriminating between '0' and '1', which requires knowledge of the wireless channel. However, brute force estimation of the threshold by taking the mean value of a series of pilot symbols with equiprobable '0's and'1's, has been used in simulation and experimental measurements and has shown similar performance to the optimal one, as shown in Fig. 4.14.

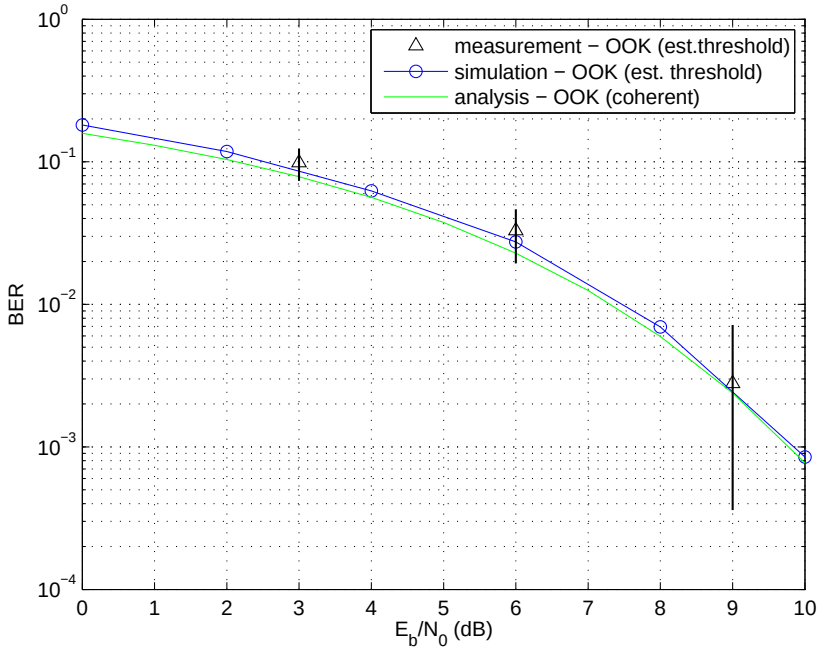

Figure 4.14: BER vs SNR for OOK.

Confidence intervals, like the ones appearing in [4], are plotted for the

experimental measurements. For N_{meas} measured bits, a Poisson distribution is assumed for the bit errors, with variance BER N_{meas}. The error bars have length of two standard deviations.

4.5.2 FSK

Probability of detection error per bit is already calculated for coherent binary FSK, and is known to perform 3dB worse than BPSK. FSK is an *orthogonal* modulation and has a distance reduced by a factor of $\sqrt{2}$ between constellation points compared to the *antipodal* BPSK ([18], Eq. 7.6.18). The BER closed form is

$$P_b^{\text{FSK, coh}} = Q\left(\sqrt{\frac{\mathcal{E}_b}{N_0}}\right), \tag{4.40}$$

where $\mathcal{E}_b = \frac{a^2}{2}T$ is the bit energy, with a being the amplitude of the bit waveform's fundamental frequency component.[3] The noise energy per bit is N_0. For non-coherent binary FSK, the BER closed form is also available ([18], Eq. 7.6.113), with its performance being inferior compared to coherent FSK, ranging from 3dB in low-SNR to about 1dB in high-SNR.

$$P_b^{\text{FSK, nc}} \approx \frac{1}{2}e^{-\frac{\mathcal{E}_b}{2N_0}} \tag{4.41}$$

Analytic, simulation and experimental measurement curves for non-coherent binary FSK are shown in Fig. 4.15, where the optimal (coherent) curve is also shown as a reference. Simulation conforms with analysis, and experimental measurements fall close to the expected curves.

[3]Bit waveforms for backscatter FSK are square pulse-trains due to transistor switch operation. A square waveform of frequency F_{sub} and amplitude 1 has a Fourier series representation $\frac{4}{\pi}\sum_{k=0}^{+\infty}\frac{1}{2k+1}cos[(2k+1)(2\pi F_{\text{sub}}t)]$ and its fundamental component's amplitude is $a = 4/\pi$. Thus, the bit energy can be expressed as $E_b = \frac{16}{\pi^2}\frac{p^2}{2}T$, where p is the tag's square waveform amplitude.

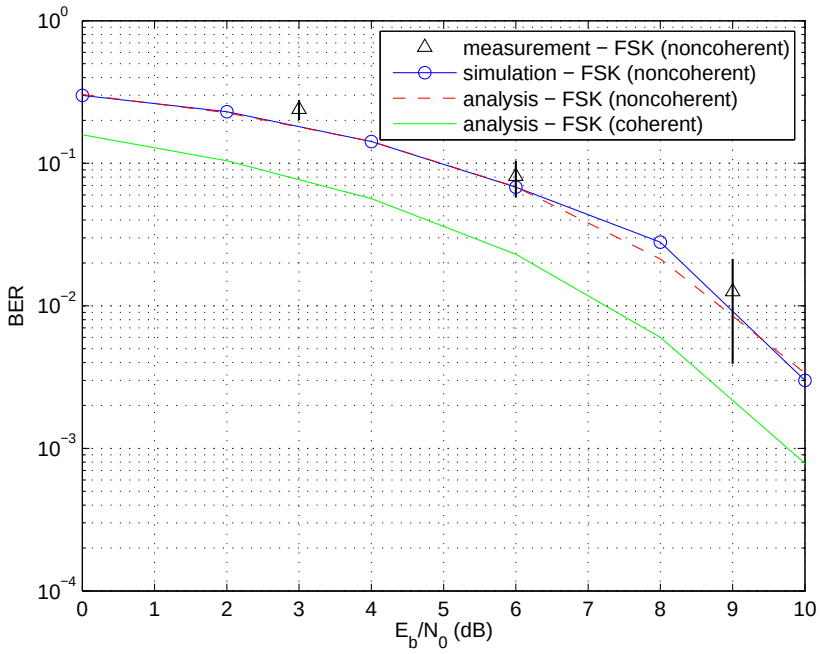

Figure 4.15: BER vs SNR for FSK.

4.6 Modulation Comparison

A comparison of the two simple modulation schemes presented is given in this section. It is shown that each modulation scheme has its advantages and drawbacks, and one should consider which one better serves the needs of a given backscatter link or network.

4.6.1 BER Performance

In Fig. 4.16, the BER curves for both non-coherent FSK and OOK are shown alongside for comparison. It can be seen that non-coherent FSK performs worse than OOK, with performance difference ranging from 3dB at SNR of 0dB to about 1dB at SNR of 10dB.

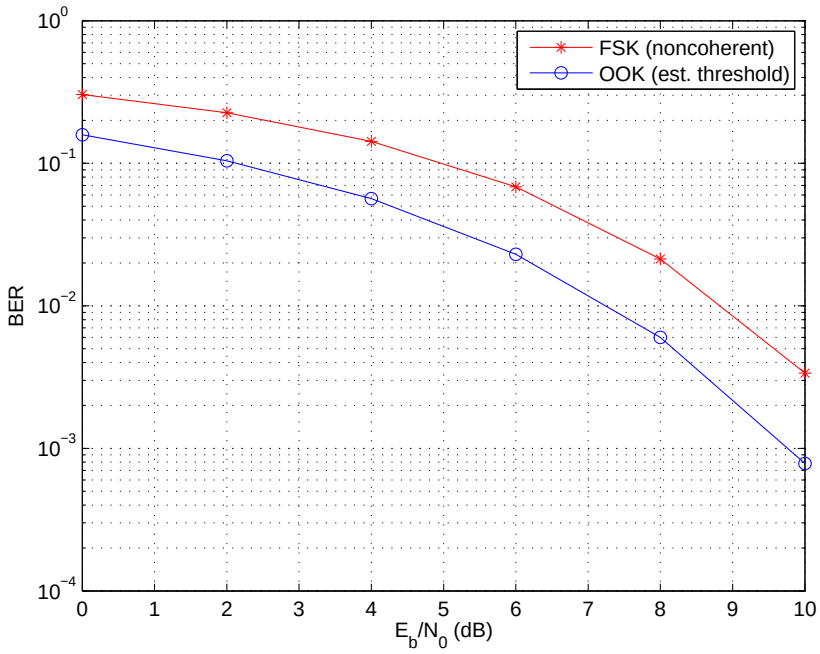

Figure 4.16: BER vs SNR for OOK and non-coherent FSK.

4.6.2 Range Performance

OOK seems to outperform non-coherent FSK if the comparison is strictly limited to BER performance. However, under careful observation of the spectrum of an OOK backscatter transmission (Fig. 4.10), it is noticed that the signal's first harmonics are very close to the carrier, even though the baudrate is high (on the order of 100kbps). This means that the backscattered signal may be overwhelmed by the carrier power if the receiver's dynamic region is not high enough. Moreover, the backscattered signal resides in a frequency region where the noise floor is elevated due to environment reflections (multipath clutter) and RF electronics get saturated by the carrier's high power due to non-linearities [28]. This effect can be observed in Fig. 4.17, where a high power carrier is transmitted and the frequency band of $866.5 - 867.5$MHz is observed with a spectrum analyzer. The increased noise power means that the SNR is lowered, and so, for a tag with a given distance from the signal generator and reader, the BER performance will be deteriorated due to

reflections. This also affects the range performance. Suppose a fixed SNR value at a given reader–tag distance d without the multi-path clutter; to achieve the same SNR when the clutter is present, the distance has to be decreased in order for the received signal's SNR to be increased. This is a great downside of the OOK modulation.

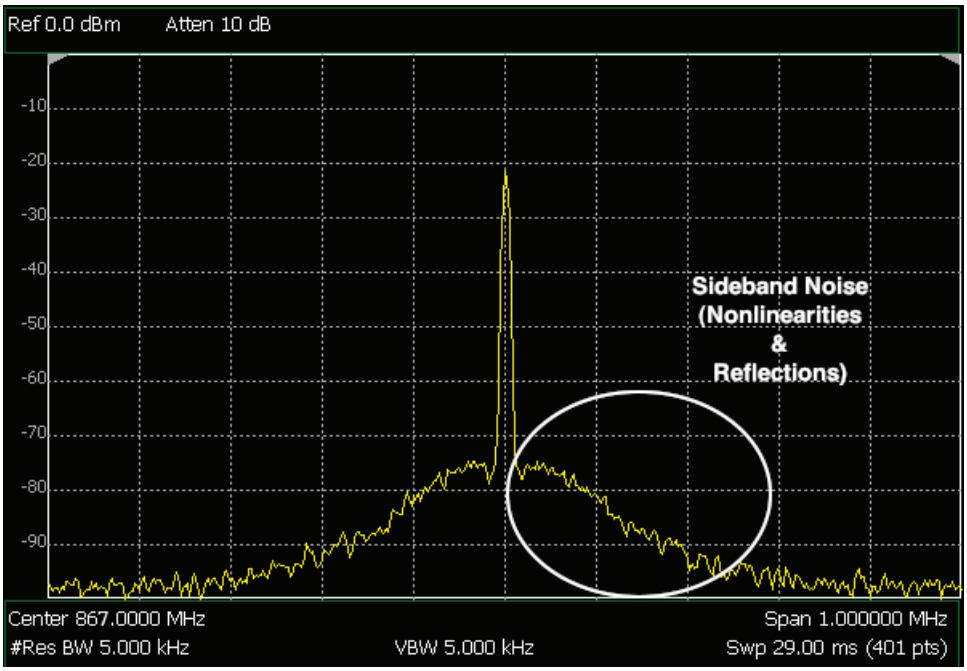

Figure 4.17: RF clutter around carrier observed with a spectrum analyzer.

A solution to the problem could be the utilization of a bistatic dislocated architecture for the reader: the signal generator is kept away from the receiving part of the reader, thus reducing the sideband noise effect in the reader caused by the generator. However, this may not always be an option. In this case, FSK modulation can be used by the backscatter link. With FSK modulation, the symbol frequencies are subcarriers that can be kept away enough from the carrier, so that they do not fall on the increased noise floor frequency region. This may be coupled with the bistatic reader architecture, to eliminate the reflections and non-linearities effect. Nevertheless, even with a collocated architecture, the effect can be minimized if the lowest subcarrier frequency is chosen to be greater than a threshold frequency. For example,

in Fig. 4.17 it can be seen that the noise floor elevation takes place up to approximately $F_c \pm 300$kHz, where $F_c = 867$MHz. In this scenario, the lowest subcarrier frequency should be above 300kHz, in order to avoid the problem.

From the above, it can be seen that one would choose OOK for increased BER performance and FSK for increased range performance. The 1dB to 3dB of performance difference between FSK and OOK can be overcome with a slight increase of the generator's output power.

4.7 Multiple Access in Backscatter Networks

A backscatter sensor system is a *network* if it makes use of some form of medium access control (MAC), or multiple access scheme. In order to ensure scalability of the whole system, hundreds of backscatter sensors have to be able to harmonically coexist in a field, all transmitting their information, without causing interference to the others. In this chapter, we present some basic concepts of multiple access in backscatter networks. Two cases are mentioned, the first being an ALOHA-style multiple access protocol where packet collisions may occur and need to be resolved via smart techniques, and the second is a frequency division multiple access (FDMA) scheme, where collisions are a priori avoided.

4.7.1 Medium Access Control - Framed ALOHA Schemes

The Generation 2 RFID Standard specifies a framed ALOHA scheme for tag inventory. The reader transmits a special *Query* command, specifying a number of slots for tag transmission. Each tag randomly selects one of the slots for transmission of a 16-bit random number (RN16). If multiple tags transmit at the same time slot, a collision occurs and the reader cannot successfully decode data. If only one tag transmits, the reader echoes back this tag's RN16 and thus acknowledging (singulating) it. Then, the tag enters

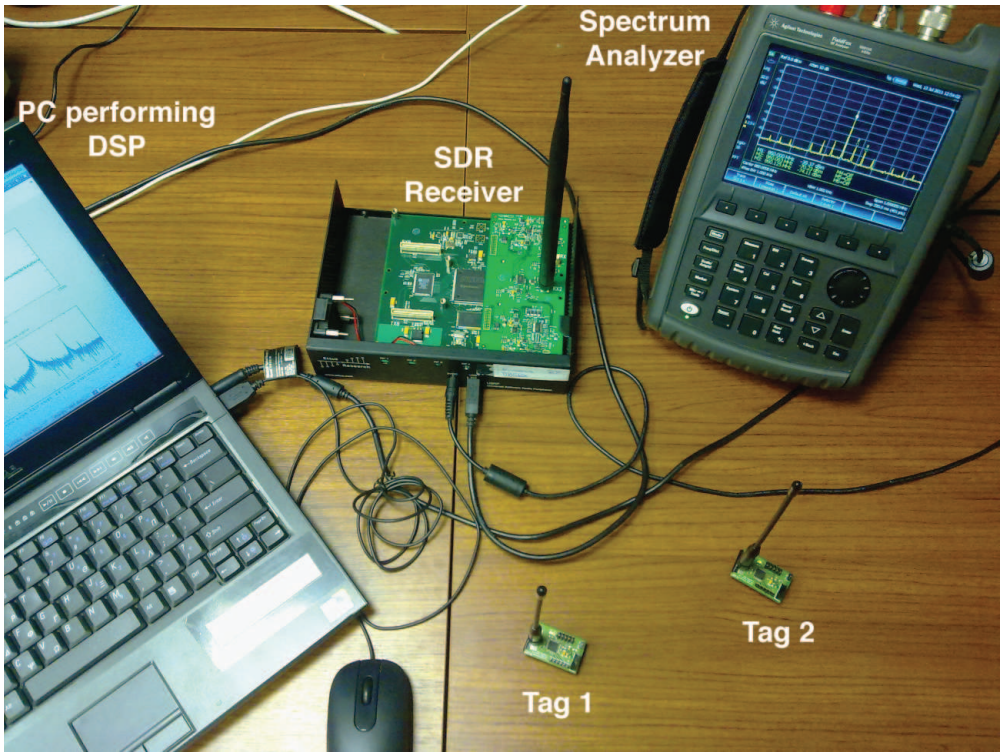

Figure 4.18: Backscatter network demo setup.

the *access* phase, where it transmits its 96-bit electronic product code (EPC) to the reader, along with additional bits for error correction, headers, etc. The reader then proceeds with the next time slot, till the frame ends. The number of time slots in a frame is adjusted at the end of each frame, by estimating the number of non-singulated tags.

In figure 4.19 an example of Gen2's MAC is shown. A reader and three tags exist in the scenario. At the beginning, the reader issues a *Query* command, advertising 2 slots for transmission, and immediately starts to transmit a continuous wave (CW). During the CW, two tags backscatter their RN16's, resulting in a collision at the reader. Because the reader can not decode the scrambled RN16s, it takes no action for them and proceeds with a *QueryRep* command, which states that a new time slot is beginning. Only one tag backscatters its RN16, which can be decoded by the reader (i.e. successful slot). The reader then issues an acknowledgement (ACK) to the tag

that was singulated and starts a CW transmission. The tag backscatters its electronic product code (EPC) and any other bits requested by the reader, and the inventory round ends.

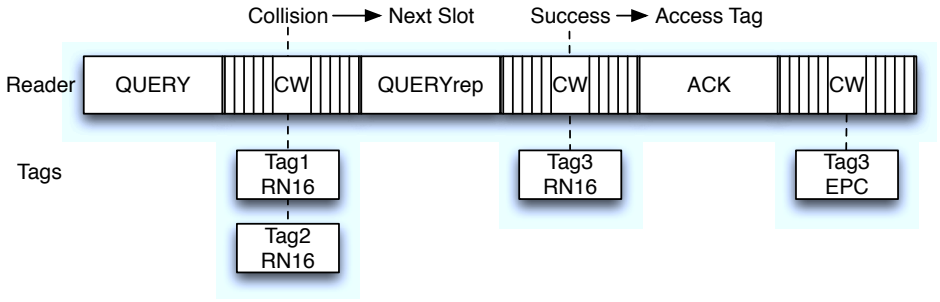

Figure 4.19: Generation 2 MAC.

Similar scenarios could be adapted to a backscatter sensor network's needs, with sensors in a backscatter cell utilizing framed ALOHA for information transmission. This of course requires that a sensor can receive reader commands, which yields the need for a receive chain on the tag's RF part, and extra processing at the sensor's MCU for command decoding, time synchronization for keeping accurate within slots, etc. Although the tag's complexity increases, this MAC scheme has the advantage of requiring a fixed amount of bandwidth for any sensor population.

Collision Detection and Decoding in ALOHA Schemes

Collisions that may occur during a Generation 2 ALOHA scheme cause the total delay for a tag population inventory to grow. If these collisions are resolved, the overall inventory delay can be reduced significantly. Although the Generation 2 standard does not specify reader-side actions in the case of a collision during the tag inventory, work has been done on collision detection on the physical layer of UHF RFID systems. Separation of RFID tag signals has been shown with multi-antenna [29] techniques. Work in [30], [31] shows single-antenna techniques for collided tags decoding, when the latter use FM0 signaling. By utilizing simple detection techniques that exploit FM0's inherent memory, the total inventory delay can be reduced by up to 17%, with no modification of the existing readers' RF front-ends.

4.7.2 Anticollision Backscatter Networks - FDMA

In cases where bandwidth is not critical, a different approach can be used for multiple access. That of frequency division multiplexing (FDM), where each sensor utilizes its own frequency band for data transmission. In environmental applications, and specifically agriculture, there is no need for high data rates, as information changes slowly with respect to time (e.g. soil humidity). This means that low-bitrate communication can be utilized, which also maximizes the possible achievable range. Low bitrates yield a narrow bandwidth, which is ideal for frequency division multiple access (FDMA) schemes, since more sensors can be fitted in a dedicated frequency band, plus the interference among the sensors is minimized.

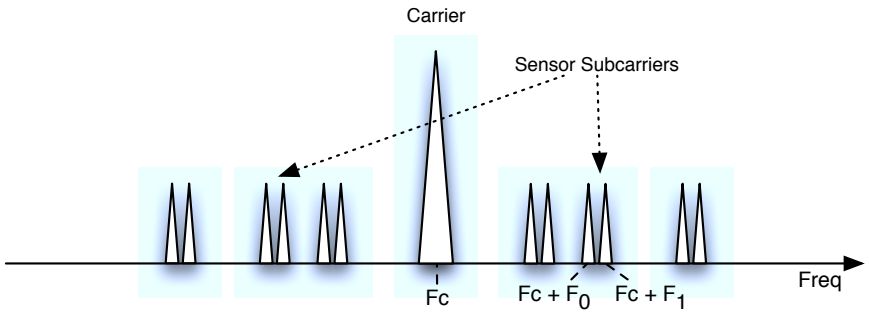

Figure 4.20: FDMA backscatter scheme.

Because only one carrier is present in the whole system (that of the signal generator), there is no way of each sensor modulating its data on its own carrier in amplitude modulation schemes. Thus, the need for a frequency modulation scheme arises. FSK modulation is ideal, as each sensor can choose unique space/mark frequencies for data transmission, which are sub-carriers of the signal generator's original carrier. Another frequency modulation, minimum shift keying (MSK), has the advantage of a fast-falling power spectrum (because of its continuous phase), meaning that interference is limited compared with FSK. By utilizing MSK modulation, even denser backscatter networks can be set up.

In FDMA schemes, collisions are *a priori* avoided if each sensor utilizes its own, unique, subcarriers, provided that they are spaced adequately so that

they do not interfere with each other (Fig. 4.20). Work has been done to quantify the probability of collision, if subcarrier frequencies are chosen randomly among sensors, depending on their population [5]. With FDMA, extra processing is done on the reader, which filters around each tag's subcarriers for information extraction. After filtering, each tag is decoded sequentially.

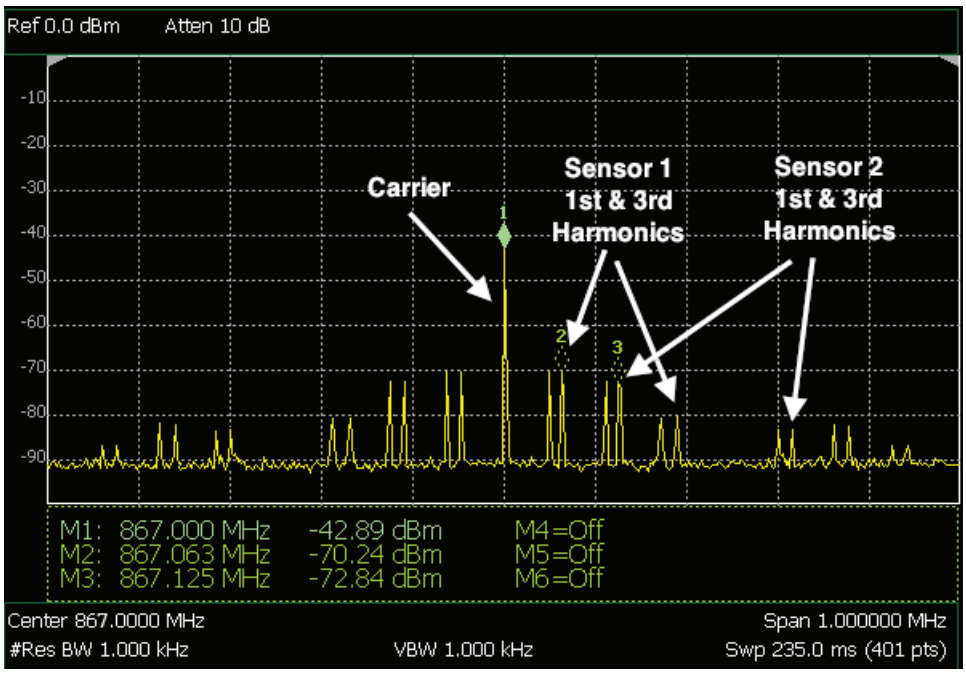

Figure 4.21: Received spectrum of two tags performing in FDMA.

Chapter 5

Conclusion, Ongoing and Future Work

Throughout this thesis, a fully functional backscatter link was designed and implemented from the ground up. Using a combination of commercial equipment for the simple functions, such as carrier generation and spectrum analysis, and custom built hardware along with the accompanying software, real-case experimentation was made. Fundamental theoretical knowledge was utilized and experimental results were compared with simulation; from the aspects of tag RF efficiency and communication schemes, to reader signal processing. A basic multiple access scheme that could perform well in backscatter sensor networks was implemented and showcased. Low-cost and low-power goals have been achieved, showing that backscatter communication can be of benefit for applications like agricultural sensing. A step has been made, towards creating a testbed for research on all parts of backscatter systems; microwave theory, circuits and hardware design, communication theory, and sensors integration.

This thesis covered the very basic of backscatter links and networks, and this work can be expanded a lot at all aspects. Some of them are mentioned below and are parts of ongoing or future work of the author and the research group he belongs to.

5.1 The Big Picture - Scalability

Backscatter is shown to be the most promising communication scheme for ultra-low cost and low power sensor networks, especially for environmental applications. Its simple, low-cost hardware will allow for hundreds of sen-

sors to coexist in a *cell*, monitoring each plant's microclimate. However, to scale the whole thing up, the backscatter cells have to be interconnected, in a similar way the GSM cells communicate with each other. Each cell's reader (or base station in GSM), could utilize an active transceiver, able to achieve a long range of communication, till the neighboring backscatter cells. This practically means employing a classic WSN as a backbone to lots of backscatter cells. Information from the WSN can be sinked to the network of networks, fulfilling the potential of backscatter networks to join the *Internet of Things* (Fig. 5.1).

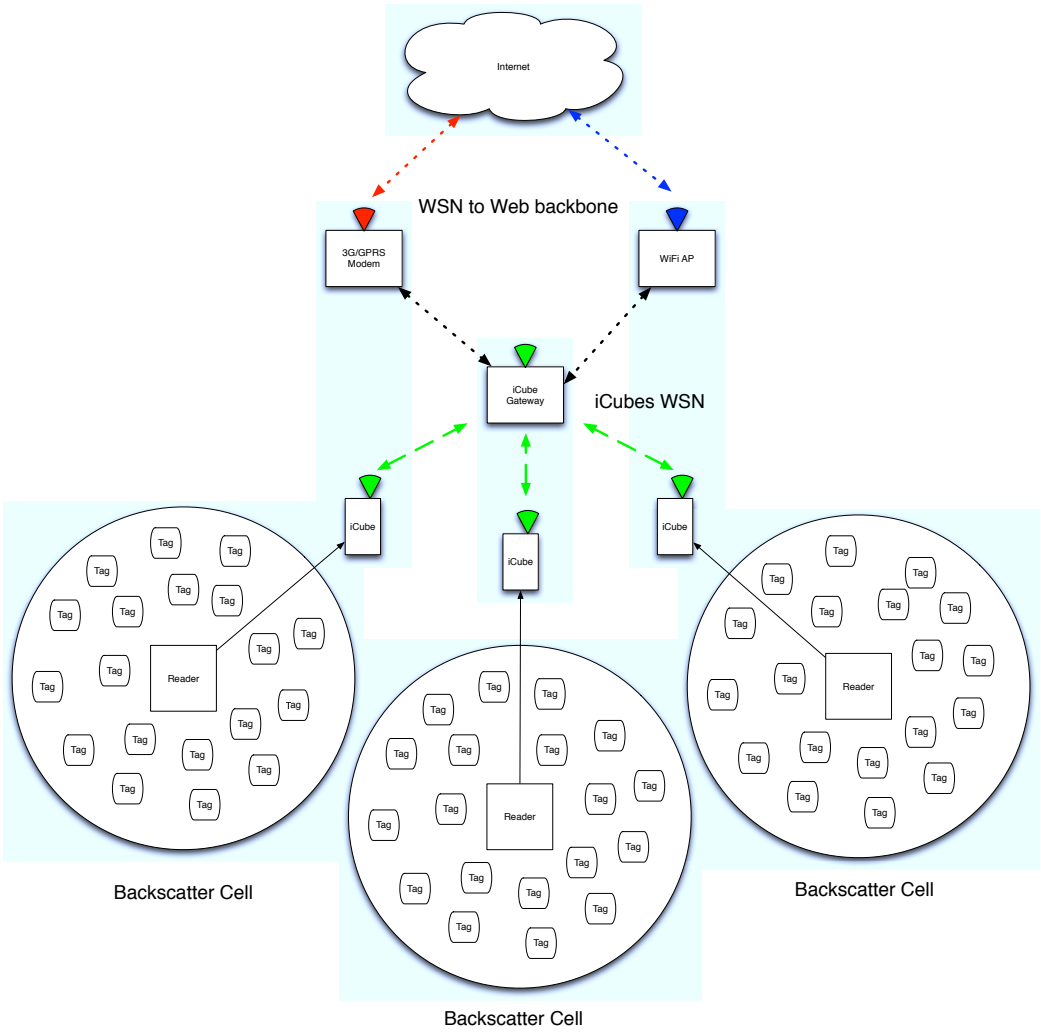

Figure 5.1: Backscatter cells connected to WSN backbone.

5.2 Power Harvesting - Renewable Energy Sources and RF Power

Due to the low-power nature of semi-passive RF tags, a small capacity battery is used, allowing the tags to wakeup, even if their distance from the reader is some decades of meters long. Even though semi-passive tags have the advantage of being independent from the reader, their batteries will sometime run low, no matter how much power their hardware dissipates. This yields the need for smart battery recharging which could be accomplished with the use of renewable energy sources such as solar panels (Fig. 5.2), or windmills. Another source of energy which could be utilized is the RF power which exists more or less everywhere at some RF band. DTV and GSM power could be harvested for slow battery charging, and create a passive–semi-passive hybrid tag [32]. This of course has to be coupled with lower consuming hardware and carefully designed software that will manage the tag's functions duty cycles properly.

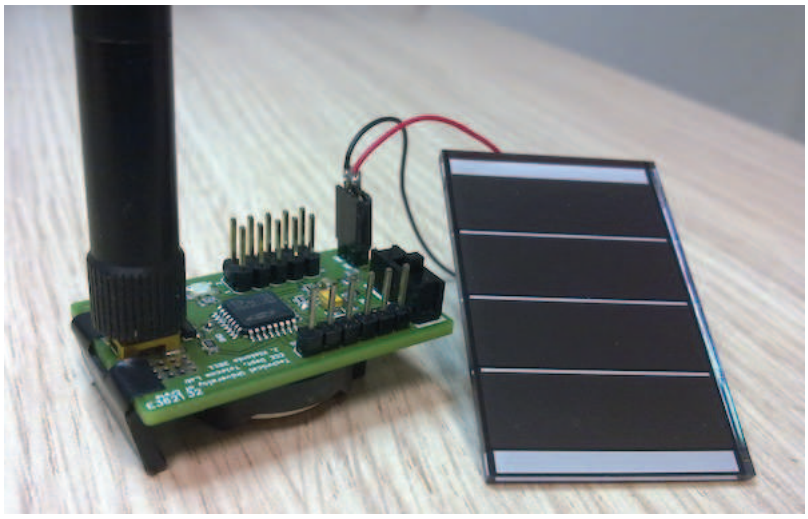

Figure 5.2: Solar panel tied to a semi-passive tag.

5.3 Range Extension

In section 3.2, the two constraints for improved backscatter communication were mentioned, but only the one for improved BER performance was exploited for the tag's RF part. The other is the constraint for maximum backscattered carrier power per bit, which is the necessary condition for maximizing the possible achievable range. This requires knowledge of the antenna *structural mode*, which can be calculated by simulation or experimental measurements. This is a crucial move for improving the tags designed in the context of this work.

The second thing to consider about the range comes from the results of range measurements of subsection 2.4.2. As can be seen, the range for tags near the signal generator is much larger compared to the ones that are lying some meters away. This is expected if we recall the simple signal model of Eq. 4.1, which states that the received backscattered signal at the reader depends on the carrier amplitude. Because the carrier suffers from the tag–reader roundtrip path loss, the backscattered signals are of low SNR. So, as far as the problem is not the reader sensitivity, more carrier generators could be utilized along with just *one* receiver for each backscatter cell. The carrier generators do not need to be expensive units, but rather cheap WSN nodes, that just transmit an unmodulated carrier whenever this is needed (e.g. when they receive a special command). The technology is there and it's cheap (Fig. 5.3).

The third thing is a challenge for backscatter networks. Current WSNs employ the principle of multihop for range extension, but could this be possible in backscatter? A tag's information which is far away from the reader and cannot be 'heard' with sufficiently high SNR, could be decoded by a tag closer to the reader, which would re-modulate and backscatter the information to the reader (Fig. 5.4). This requires a receive chain for each tag, and more complex software running on them.

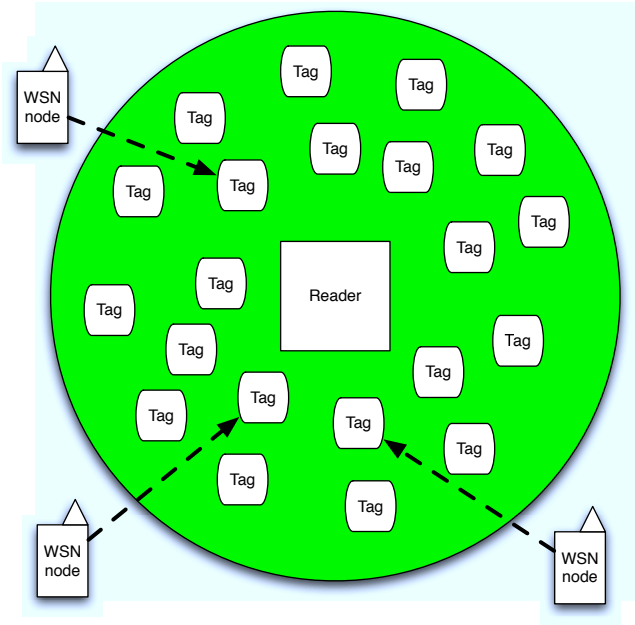

Figure 5.3: Hybrid backscatter field.

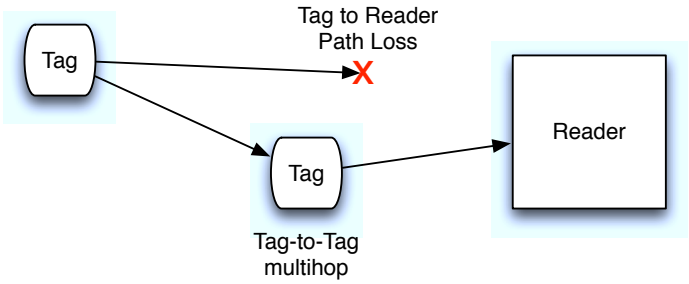

Figure 5.4: Multihop backscatter scheme.

5.4 MCU-less Sensors

Another challenge for backscatter sensors is to simplify not only their communication part, but also their processing hardware. By omitting the MCU and using simplified circuitry for sensor interfacing with the tag's RF part, cost, complexity and power demands are reduced. Such a prototype design can be seen in Fig. 5.5, where the capacitive humidity sensor described in [3] is interfaced directly to a RF transistor driving the tag's antenna. The frequency output from the sensor resonant circuitry switches the RF transistor

at a frequency proportional to the environment's relative humidity ($\%RH$). This results in an analog frequency modulation (FM) spectrum, as shown in Fig. 5.6. The information can be decoded by finding the peak of the FFT of the received signal. The challenges, however, with such a design are how a multiple access scheme can be implemented, and how such a sensor can be selectively waked up by the reader, without very complex circuitry, since no MCU is present for additional control of those two.

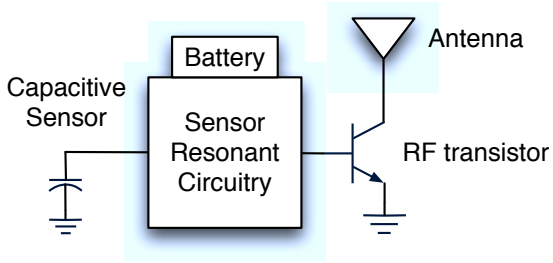

Figure 5.5: MCU-less semi-passive sensor prototype design.

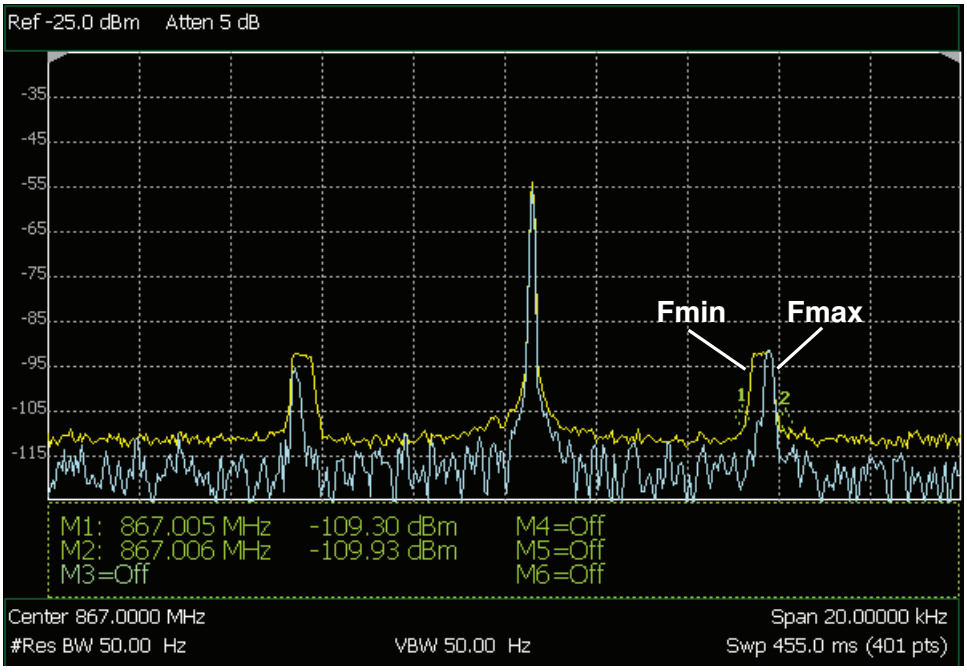

Figure 5.6: Analog FM spectrum of MCU-less sensor.

5.5 Software Defined Reader RF Front-End Improvements

One of the main future objectives is the design of a custom RF front-end for the software defined reader. Because of the nature of backscatter radio, where the operating SNR is always low, a sensitive super-heterodyne receiver is needed for the reader. Its operation should be limited to the UHF ISM bands for Europe and the US with narrowband selective components, to achieve a good sensitivity level and low noise figure (NF). The RF front end should be interfaced to ADC and DAC converters and route the digitized data to MATLAB for signal processing.

Appendix 1

Semi-passive Tag PCB Layout and Schematic

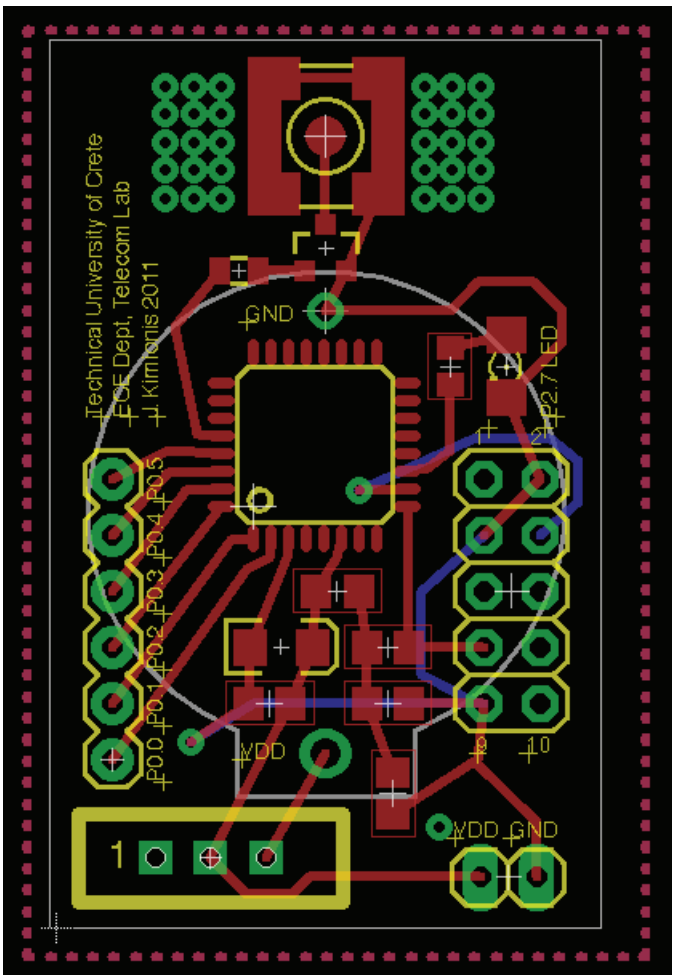

Figure 5.7: Semi-passive tag PCB layout.

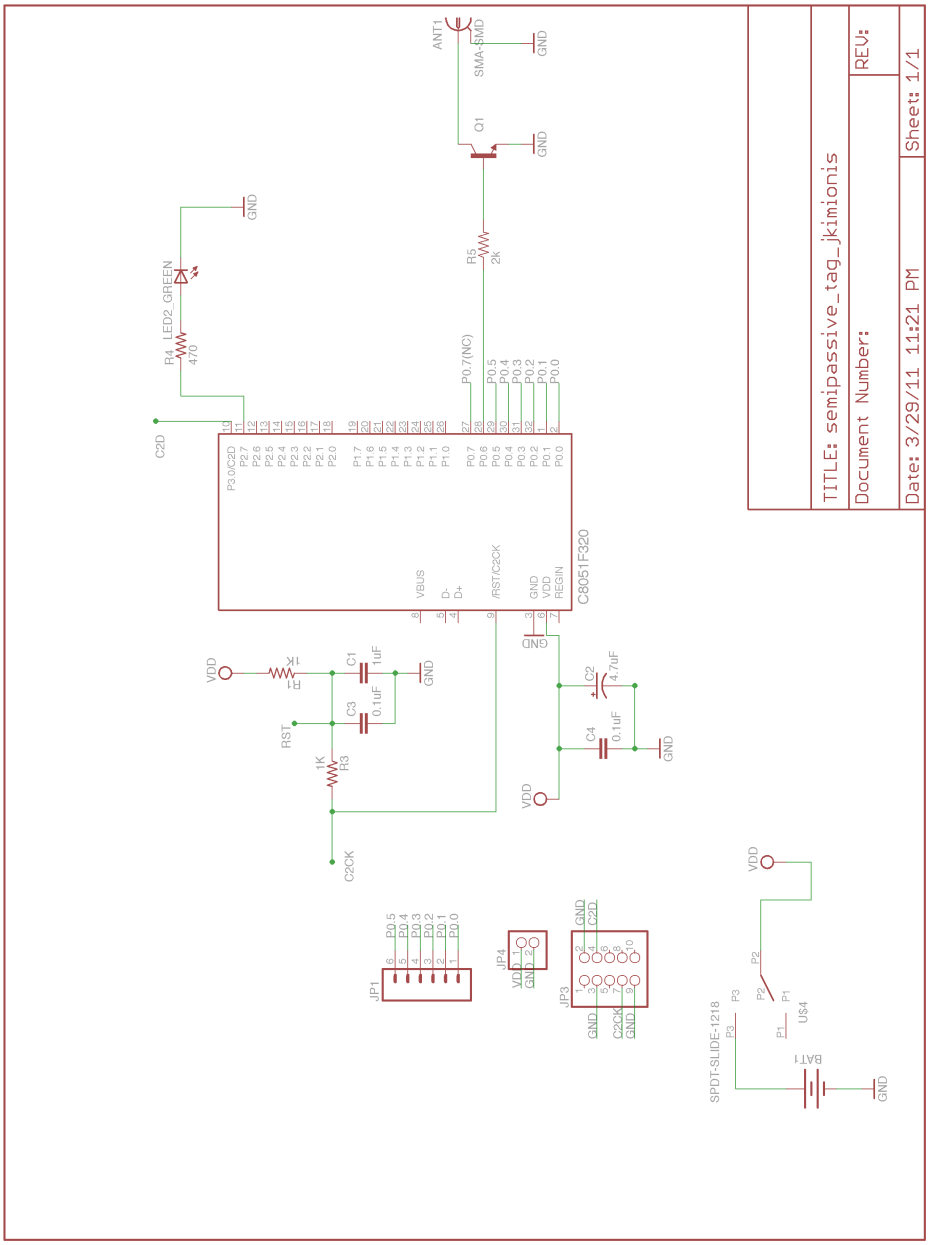

Figure 5.8: Semi-passive tag schematic.

Appendix 2

Communication Software Routines

Below, the main function and interrupt service routines (ISR) for the software's communication part (FSK modulation) are presented in pseudocode. Implementation for most MCUs should be straightforward. Two timers are utilized; the SUBCARRIER_TIMER and the BIT_TIMER. The bits for transmission are kept in the txData buffer, and the transistor's gate is controlled by the pin called GATE. The first example utilizes two subcarrier frequencies, with $F_1 = 2F_0$. See subsection 3.4.2 for details.

```
txData[] = {0, 0, 1, 0, 1, 1};

sendPacket() {
    counter = 0;                    // reset subcarrier counter
    index = 0;                      // reset txData index
    BIT_TIMER_RUN();                // start the bit duration timer
    while(transmitting) {           // while the busy flag is on
            ;                       // wait
    }
}

SUBCARRIER_TIMER_ISR() {
    if(bit_value == 1) {            // if bit 1
            GATE = !GATE;           // switch at full rate
    }
    else {                          // if bit 0
       if(counter % 2 == 0) {       // switch at half rate
          GATE = !GATE;             // (at even counter values)
       }
       counter = !counter;          // toggle the counter 0 <-> 1
```

```
    }
}

BIT_TIMER_ISR() {
    if(index > length(txData) - 1) {// if txData ended
        SUBCARRIER_TIMER_STOP();  // stop the subcarrier timer
        BIT_TIMER_STOP();         // stop the bit duration timer
        transmitting = 0;         // unset the busy flag
        GATE = 1;                 // set transistor
    }
    bit_value = txData[index];    // set the bit value
    index++;                      // increment index
    counter = 0;                  // reset the subcarrier counter
    if(index == 1) {              // if transmission started now
        SUBCARRIER_TIMER_RUN();   // start the subcarrier timer
        transmitting = 1;         // set the busy flag
      }
}
```

The second example shows the case where the subcarrier timer is reprogrammed each time, to meet the bit waveform's frequency. This technique allows higher control over the selection of the subcarrier frequencies for each tag. To generate a frequency F_{sub} (kHz), the subcarrier timer's period has to be programmed to $\frac{10^3}{2F_{\text{sub}}}(\mu s)$.

```
txData[] = {0, 0, 1, 0, 1, 1};

sendPacket() {
    transmitting = 1;             // set the busy flag
    index = 0;                    // reset txData index
    bit_value = txData[index];    // load first bit

    if(bit_value == 0) {
        SUBCARRIER_TIMER_PERIOD_US(2);     // 250kHz subcarrier
    }
    else {
        SUBCARRIER_TIMER_PERIOD_US(1.25); // 400kHz subcarrier
    }
```

```
    SUBCARRIER_TIMER_RESET();       // zero the timer counter
    RESET_BIT_TIMER_RESET();        // zero the bit duration timer

    SUBCARRIER_TIMER_RUN();         // start the subcarrier timer
    BIT_TIMER_RUN();                // start the bit duration timer

    while(transmitting) {           // while the busy flag is on
            ;                       // wait
    }
}

SUBCARRIER_TIMER_ISR() {
    GATE = !GATE;                   // switch transistor
}

BIT_TIMER_ISR() {
    if(index > length(txData) - 1) {// if txData ended
        SUBCARRIER_TIMER_STOP();    // stop the subcarrier timer
        BIT_TIMER_STOP();           // stop the bit duration timer
        transmitting = 0;           // unset the busy flag
    }
    index++;                        // increment index
    bit_value = txData[index];      // set the bit value

    if(bit_value == 0) {
        SUBCARRIER_TIMER_PERIOD_US(2);     // 250kHz subcarrier
    }
    else {
        SUBCARRIER_TIMER_PERIOD_US(1.25); // 400kHz subcarrier
    }

}
```

Bibliography

[1] H. Stockman, "Communication by means of reflected power," *Proc. IRE*, pp. 1196–1204, 1948.

[2] D. M. Dobkin, "The RF in RFID: Passive UHF RFID in Practice," Newnes (Elsevier), 2008.

[3] A. Bletsas, A. Vlachaki, E. Kampianakis, G. Sklivanitis, J. Kimionis, K. Tountas, M. Asteris and P. Markopoulos, "Towards Precision Agriculture: Building a Soil Wetness Multi-Hop WSN from First Principles", in *Second International Workshop in Sensing Technologies in Architecture, Forestry and Environment (ECOSENSE) 2011, Belgrade, Serbia*, Apr. 2011.

[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, June 2008.

[5] A. Bletsas, S. Siachalou, and J. N. Sahalos, "Anti-collision backscatter sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5018–5029, Oct. 2009.

[6] A. Ferrer-Vidal, A. Rida, S. Basat, L. Yang, and M. M. Tentzeris, "Integration of Sensors and RFIDs on Ultra-low-cost Paper-based Substrates for Wireless Sensor Networks Applications," in *Procs. of the 2006 2nd Workshop on Wireless Mesh Networks (WiMesh 2006)*.

[7] M. A. Green, K. Emery, Y.Hishikawa, and W. Warta, "Solar Cell Efficiency Tables (v.37)," *Progress in Photovoltaics: Research and Applications*, vol. 19, pp. 84–92, Dec. 2010.

[8] S. Roundy, "On the Effectiveness of Vibration-based Energy Harvesting," *Journal of Intelligent Material Systems and Structures*, vol. 16, no. 10, pp. 809–823, Oct. 2005.

[9] A. Georgiadis, G. Andia, and A. Collado, "Rectenna Design and Optimization Using Reciprocity Theory and Harmonic Balance Analysis for Electromagnetic (EM) Energy Harvesting," *IEEE Antennas and Wireless Propagation Letters*, vol. 9, pp. 444–446, July 2010.

[10] A. Bletsas, A. G. Dimitriou, and J. N. Sahalos, "Improving backscatter radio tag efficiency," *IEEE Trans. Microwave Theory Tech.*, vol. 58, no. 6, pp. 1502–1509, June 2010.

[11] J. D. Griffin and G. D. Durgin, "Complete link budgets for backscatter-radio and RFID systems," *IEEE Antennas Propag. Mag.*, vol. 51, no. 2, pp. 1125, Apr. 2009.

[12] M. Buettner and D. Wetherall, "A Gen 2 RFID monitor based on the USRP," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 3, pp. 42–47, July 2010.

[13] "EPC Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHZ-960 MHZ, version 1.2.0," EPC Global, 2008.

[14] Silicon Labs C8051F320/1 manual, *available online*.

[15] Silicon Labs C8051F320DK manual, *available online*.

[16] Texas Instruments, "Designer's Guide to LPRF," *available online*.

[17] A. Bletsas, A. Vlachaki, E. Kampianakis, J. Kimionis, G. Sklivanitis, K. Tountas, M. Asteris, and P. Markopoulos, "Building the Low-Cost Digital Garden as a Telecom Lab Exercise," *IEEE Pervasive Computing,* submitted for publication, Aug. 2010, Accepted on Oct. 2011, to appear in 2012.

[18] J. G. Proakis and M. Salehi, "Communication Systems Engineering," *Prentice-Hall International, Inc.*, 2001.

[19] Ettus Research, Universal Software Radio Peripheral, http://www.ettus.com.

[20] Tools4SDR, http://www.tools4sdr.com.

[21] S. Aja-Fernandez, C. Alberola-Lopez, and C. Westin, "Noise and Signal Estimation in Magnitude MRI and Rician Distributed Images: A LMMSE Approach," *IEEE Transactions on Image Processing*, vol. 17, no. 8, pp. 1383–1398, August 2008.

[22] J. Sijbers, A. Den Dekker, A. J. Den Dekker, P. Scheunders, and D. Van Dyck, "Maximum-Likelihood Estimation of Rician Distribution Parameters," *IEEE Transactions on Medical Imaging*, vol. 17, pp. 357–361, 1998.

[23] H. Gudbjartsson and S. Patz, "The Rician distribution of noisy MRI data," *Magnetic Resonance in Medicine*, vol. 34, pp. 910–914, 1995.

[24] A. P. Liavas, "Communication Systems II" (Course Notes), at the *Electronic and Computer Engineering Dept., Technical University of Crete*, Spring 2010.

[25] C. R. Johnson and W. A. Sethares, "Telecommunications Breakdown: Concepts of Communication Transmitted via Software-Defined Radio," *Prentice Hall International, Inc.*, 2003.

[26] Suckchel Yang, Jung-wan Park, Yong Moon, Won Cheol Lee, and Yoan Shin, "A Noncoherent UWB Communication System for Low Power Applications," *Journal of Semiconductor Technology and Science*, vol. 4, no. 3 pp. 210–216, Sept. 2004.

[27] M. Simon and D. Divsalar, "Some interesting observations for certain line codes with application to rfid," *IEEE Trans. Commun.*, vol. 54, no. 4, pp. 583–586, Apr. 2006.

[28] B. Razavi "RF Microelectronics," *Prentice-Hall International, Inc.*, 1998.

[29] B. Frey, "Source separation for UHF RFID," M.S Thesis, Delft and ETH, 2008, mentor Geert Leus, supervisor Helmut Bölcskei.

[30] J. Kimionis, A. Bletsas, A.G. Dimitriou, and G.N. Karystinos, "Inventory Time Reduction in Gen2 with Single-Antenna Separation of FM0 RFID signals," in *IEEE International Conference on RFID-Technology and Applications (RFID-TA) 2011*, Sitges, Barcelona, Spain, Sept. 2011.

[31] A. Bletsas, J. Kimionis, A. G. Dimitriou, and G. N. Karystinos, "Single-antenna coherent detection of collided FM0 RFID signals," *IEEE Transactions on Communications,* submitted for publication, Apr. 2011, accepted on Nov. 2011, to appear in 2012.

[32] C. Mikeka, H. Arai, A. Georgiadis, and A. Collado, "DTV Band Micropower RF Energy-Harvesting Circuit Architecture and Performance Analysis," in *IEEE International Conference on RFID-Technology and Applications (RFID-TA) 2011*, Sitges, Barcelona, Spain, Sept. 2011.