BLISP: Enhancing Backscatter Radio with Active Radio for Computational RFIDs

Ivar in ’t Veen
BLISP: Enhancing Backscatter Radio with Active Radio for Computational RFIDs

Master's Thesis in Embedded Systems

Embedded Software Section
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology
Mekelweg 4, 2628 CD Delft, The Netherlands

Ivar in’t Veen
I.J.G.intVeen@student.tudelft.nl

Friday 27th November, 2015
This project was partly funded by the KIVI travel grant and the Embedded Software Group at Delft University of Technology. Their contribution is hereby gratefully acknowledged.

The content of this thesis is being submitted as the article titled “BLISP: Enhancing Backscatter Radio with Active Radio for Computational RFIDs” by Ivar in’t Veen, Qingzhi Liu, Przemyslaw Pawelczak, Aaron Parks, and Joshua R. Smith to IEEE RFID 2016.

The ideas presented in this thesis are part of the patent application (application number 20154320) “Method of transmitting data from a mobile transmitter device to a host unit, and mobile transmitter device” filed on 14th September 2015.
Author
Ivar in’t Veen (I.J.G.intVeen@student.tudelft.nl)

Title
BLISP: Enhancing Backscatter Radio with Active Radio for Computational RFIDs

MSc presentation
Friday 27th November, 2015

Graduation Committee
Prof. dr. K.G. Langendoen (Chair) Delft University of Technology
dr. Przemysław Pawelczak (Supervisor) Delft University of Technology
dr. Alberto Bacchelli (External member) Delft University of Technology
Qingzhi Liu, MSc Delft University of Technology
Abstract

With the rise of the Internet of Things (IoT) there is an growing need for energy efficient wireless communication methods. Most radio technologies can be divided into two groups: passive/backscatter and active radio. As representatives of these techniques we evaluate the Wireless Identification and Sensing Platform (WISP) an EPCglobal Class 1 Generation 2 Radio Frequency Identification (RFID) standard-based, Computational RFID backscatter radio, against Bluetooth Low Energy (BLE). In this thesis we show (theoretically and experimentally) that WISP in high channel attenuation conditions is less energy efficient per transmitted byte than BLE active radio. BLE is shown to be less energy efficient in the short range while being the only viable option in the longer range. Exploiting this observation we design a simple switching mechanism that backs off to BLE when radio conditions for WISP are unfavorable. In consequence we demonstrate world’s first hybrid radio platform which combines the strengths of active radio (long range and robustness to interference) and backscatter radio (low power consumption and independency of battery supply). By a set of laboratory experiments we show that our proposed hybrid active/backscatter radio obtains higher goodput than WISP and lower energy consumption than BLE as stand-alone platforms. These results especially hold when WISP is in range of an RFID-reader for the majority of time. At the same time our proposed platform is as energy efficient as BLE when user is mostly out of RFID-reader range.

Keywords: Backscatter, Radio Frequency Identification, Bluetooth Low Energy, Channel Estimation, Multi-Radio Switching, Energy
Acknowledgements

First, I would like to thank Przemyslaw Pawelczak for being an inspirational and optimistic guide during my thesis project. Also I would like to thank Qingzhi Liu for his guidance and discussions regarding this project. I would also like to thank Marco Cattani and Ioannis Protonotarios for creating ‘Gondola’ as it improved the replicability of our measurements. Words of acknowledgment go to the Embedded Software Group at Delft University of Technology for their feedback and help in realizing this work.

The work presented in this thesis was partly done at the Sensor Systems Laboratory of the University of Washington (Seattle, WA, USA). I would like to especially thank Joshua R. Smith, Aaron Parks and all the other people for their input and guidance.

Many thanks go out to my family and friends for their distraction, encouragement and helpful input. Finally, I want to thank everybody who proofread this thesis for their input.
Preface

This document in front of you is the Master Thesis I wrote as final part of the Master of Science in Embedded Systems program I followed at Delft University of Technology.

It was at the Internet of Things seminar course, part of my master curriculum, that I first learned about the ambient backscatter phenomenon. The possibility for wireless communication using a battery-less device, by [1] referred to as “Communication out of Thin Air”, immediately tickled my imagination. When searching for a Master thesis subject I came across the opportunity to work on a closely related technology—the WISP (Computational RFID) backscatter platform.

The Wireless Identification and Sensing Platform (WISP) backscatter platform we used in this thesis is an open-source project. While developing software for our project, we regularly contributed fixes and new features back to the community. It was my first real collaboration to an open-source project, a positive experience.

Ivar in’t Veen

Delft, The Netherlands

Friday 27th November, 2015
Contents

Acknowledgements v
Preface vii
List of Acronyms xi

1 Introduction 1
1.1 Problem Statement ................................. 2
1.2 Research Question ................................. 2
1.3 Contributions ...................................... 3
1.4 Thesis Organisation ............................... 4

2 Active versus Backscatter Radio: Energy/Range Trade-Offs 5
2.1 Active Radio ..................................... 5
2.2 Passive/Backscatter Radio ......................... 6
2.2.1 Radio Frequency Identification ............... 6
2.2.2 Computational RFID ......................... 6
2.3 Analysis ......................................... 7
2.4 Measurement .................................... 8
2.4.1 Bluetooth Low Energy—Transmitter/Receiver . 8
2.4.2 Computational RFID—Transmitter/Receiver ... 9
2.4.3 Measurement Setup ........................... 9
2.4.4 Measurement Results ....................... 10
2.5 Solution: Multi-Radio Systems ................. 12
2.6 Alternative Solutions ......................... 12
2.6.1 Low Power Active Radio with Battery ....... 12
2.6.2 Power Harvester with Active Radio .......... 13
2.6.3 Backscatter Radio with Improved Channel Coding ... 13
2.6.4 Improved Energy Harvesting for CRFID ..... 13
3 BLISP: Architecture and Implementation

3.1 BLISP Hardware Architecture

3.1.1 Radio Collaboration

3.1.2 Energy Harvester

3.1.3 BLISP Receiver/Sink

3.2 BLISP Software Architecture

3.2.1 Wireless Identification and Sensing Platform

3.2.2 Bluetooth Low Energy

3.3 Backscatter Channel Estimation

3.3.1 Classical Estimation Methods

3.3.2 Proposed Estimation Method

3.4 Radio Switching

3.4.1 Random (< x)

3.4.2 Naïve

4 BLISP: Experimental Evaluation

4.1 Experiment Setup

4.1.1 Measurement Replicability

4.1.2 Data Acquisition

4.2 Static RFID Reader Experiment

4.3 Mobile RFID Reader Experiment

5 Summary

5.1 Limitations

5.2 Future Work

5.3 Conclusions

A BLISP PCB

B BLISP Firmware

B.1 Random Number Generation

B.1.1 Offline–Random Data Generation

B.1.2 Online–Random Number Generator

B.2 Message Formats

B.2.1 WISP to BLE

B.2.2 Bluetooth Low Energy (BLE) Advertising

B.2.3 WISP to Host
List of Acronyms

ACK    Acknowledgement
ADC    Analog to Digital Converter
API    Application Programable Interface
BLE    Bluetooth Low Energy
BLISP  platform combined of BLE and WISP
COTS   Commercial of-the-Shelf
CRFID  Computational RFID
DUT    Device Under Test
EPC C1G2 EPCglobal Class 1 Generation 2
EPC    Electronic Product Code
FRAM   Ferroelectric Random Access Memory
GPIO   General Purpose Input/Output
GSM    Global System for Mobile communication
IDE    Integrated Developement Environment
IoT    Internet of Things
LLRP   Low-Level Reader Protocol
LSB    Least Significant Bit
OCR    Optical Character Recognition
PCB    Printed Circuit Board
RFID   Radio Frequency Identification
RF     Radio Frequency
RN16   16bit Random Number
RSSI   Received Signal Strength Indication
SoC    System on Chip
UART   Universal Asynchronous Receiver/Transmitter
USB    Universal Serial Bus
WISP   Wireless Identification and Sensing Platform
Chapter 1

Introduction

The majority of low power wireless sensors use active radio transmission techniques, such as Bluetooth Low Energy [2], to transport data. While active radios are becoming more efficient with each year (in terms of throughput and range), the power consumption spend by wireless radios can still be orders of multitude larger than the power consumption spent for computations [3].

This proves that there is still a lot to be done to make wireless sensors more power efficient, despite many years of research in low power electronics. Most low power radio platforms try to solve the power consumption issue by limiting transmission power, limiting transmission duty cycles, limiting protocol overhead, improving receiver sensitivity or decreasing susceptibility to interference by adding extensive channel coding mechanisms. While all these methods indeed improve radio performance compared to energy consumption they are still based on active transmission of radio waves.

Another different approach to reduce energy consumption of the wireless front end is by not actively transmitting, but instead reflecting and modulating energy emitted by the transmitter—as with Radio Frequency Identification (RFID)-based Computational RFIDs (CRFIDs) [4].
1.1 Problem Statement

Unfortunately the transmission technique used by CRFIDs, i.e. backscatter, has less ideal characteristics compared to the active radios. Simply, backscatter communication, while power efficient, is very easy to distort by external or environmental influences [5, Fig. 4].

Firstly, the path loss for backscatter signals is very different than for active transmissions. Active transmissions have a signal to noise ratio which approximately decays with the square of distance. For backscatter radio this decay approximates the fourth power of distance [5, Sec. 2.2].

Secondly, reflections of active transmitted signals may result in constructive interference in which two waves collide and add up. There is no such constructive interference with backscatter signals, as reflections will always be based on the stronger original carrier wave. Therefore, collisions will always be destructive. Hence, the energy wasted by lost transmission increases.

At the same time active radios, although more resistant to interference, consume more energy than backscatter radios. The difference in power consumption is mostly due to the need to actively produce new RF waves instead of reflecting already existing ones.

1.2 Research Question

The robustness/energy efficiency trade-off of active and backscatter radio calls to connect these two platforms and find out if this combination can indeed mitigate this trade-off.

This leads us to the following research question:

\textbf{What energy consumption and transmission reliability improvements can one get exploiting the combined benefits of active and backscatter radio?}
1.3 Contributions

To answer this question we design a new heterogeneous radio sensor node combining both active and passive radio into one device. We call this platform BLISP—a composition of Bluetooth Low Energy (state of the art Commercial of-the-Shelf (COTS) active radio platform for consumer applications [2]) and WISP [6] (state of the art CRFID).

This proposed platform consists both of a low-cost experimental hardware platform connecting the two radios into one system. The platform includes a feedback-less backscatter channel estimation method and software based radio switching technique. The goal of the channel estimating switch is to choose the appropriate radio for the appropriate situation trying to optimize both reliability and energy efficiency.

To show the benefit of our proposed heterogeneous radio platform the complete system is evaluated in replicable static and mobile scenarios for both a COTS RFID reader and a modified smartphone-attached RFID reader.

The contributions presented in this thesis are:

Contribution 1: we provide a set of simple theories, supported by experiments, showing the benefit of connecting active and backscatter radio platforms;

Contribution 2: we show the benefit of using BLISP as an extension to CRFID applications by demonstrating that it is possible to transmit infinitely more data compared to an out of range CRFID while only increasing energy consumption per byte by \(\approx 15\%\) compared to Bluetooth Low Energy (BLE);

Contribution 3: we show the benefit of using BLISP as an extension to BLE applications by demonstrating that it is possible to transmit the same amount of data compared BLE while decreasing energy consumption per byte by more than 50\% compared to BLE.
1.4 Thesis Organisation

The rest of the thesis is organized as follows. Chapter 2 introduces active and passive radio techniques and explain (theoretically and experimentally) why it is not a satisfactory solution to only use one of the two in isolation. Chapter 3 discusses the hardware and software design of BLISP, including a proposal for feedback-less backscatter channel estimation and a active/passive radio switching method. In Chapter 4 the BLISP is experimentally showning to improve data rate and energy efficiency beyond the sum of the components. Finally Chapter 5 lists system limitations, ideas for research and future work, and concludes this thesis.
Chapter 2

Active versus Backscatter Radio: Energy/Range Trade-Offs

Before introducing BLISP we need to understand the trade-offs between active and backscatter radio. We define two types of radio techniques: passive/backscatter radio and active radio. First, both backscatter radio and active radio are introduced in Sections 2.1 and 2.2. Section 2.3 defines a theoretical basis for defining and evaluating energy/range trade-off. In Section 2.4 these theories are evaluated against measurement. Finally the chapter is concluded by reviewing related radio efficiency solutions in Section 2.6.

2.1 Active Radio

Classically wireless radios actively radiate RF energy waves in order to transfer data. Active (low power) radio systems are less susceptible to interference compared to backscatter communication, however, bringing the disadvantage of higher energy consumption. There are multitude of low power active radio platforms and this chapter is too short to review them all. For example, recent standards like SigFox [7], LoRa [8] or IEEE 802.15.4k [9] could be used, expected to have very low energy consumption. We are not using them in this work as they are not (yet) easily accessible for experimental evaluation, nor broadly adopted by the consumers. In special, there is an active radio platform believed to be broadly adopted, with more than 30 billion devices expected to reach the consumer market by 2020 [10]: Bluetooth.
More recently a special low power variant called BLE [10] was introduced to support the Internet of Things (IoT) and mainly focuses on control and monitoring applications. BLE operates in the 2.4 GHz band, has 40 channels, a maximum data rate of 1 Mbps and a maximum advertising payload of 47 Bytes. For the interested reader, works by [2] and [11] experimentally evaluate the performance of BLE, while [12] shows the energy consumption of BLE compared to other popular active radio technologies. Unfortunately, it is not yet known how the energy consumption of BLE compares against a CRFID.

2.2 Passive/Backscatter Radio

Originating in radar technologies from around World War II [13], passive (or backscatter) radio provides a different kind of wireless data communication. Instead of relying on the active creation and transmission of radio waves backscatter radio modulates data on top of existing RF waves.

2.2.1 Radio Frequency Identification

The most broadly known and accepted implementation of backscatter communication is known as RFID. RFID is currently mainly being used to provide unique identification numbers for access control and more recently payment of public transport and small purchases.

The EPCglobal Class 1 Generation 2 (EPC C1G2) protocol [14] is one of the main RFID protocols currently in use by industry. This standard focuses on identification and storage of small amounts of data. The US version of EPC C1G2 standard used in this work operates in the 960 MHz band, has 50 channels and relies on slotted ALOHA to mitigate the risk of collisions.

2.2.2 Computational RFID

The use of Computational RFID (CRFID) for wireless sensor applications has been advocated by many papers including [15] and [16]. The only stable CRFID [4] implementation currently available is the Wireless Identification and Sensing Platform (WISP). The communication protocol used by WISP is the industrial standard EPC C1G2 RFID-protocol.

Although completely battery-autonomous, CRFID has its intrinsic limitations. The main being limited channel robustness, as evaluated by [5], and limited RF power transfer efficiency and therefore intermittent power supply.
A solution to the problem of continuous power supply proposed by [17] exercises a hybrid power solution based on an RF power harvester and an energy storage device. While this significantly improves CRFID performance, the communication channel is still far from robust requiring further improvements to the CRFID architecture.

2.3 Analysis

To understand why CRFID is not the most energy efficient radio platform for all situations we introduce a simple analytical framework which will bring insight into the design of BLISP. We shall form a theoretical model first, followed by experimental results verifying the theory.

Assume a hybrid radio platform composed of \( i = \{1, n\} \) independent radio technologies (such as backscatter and active radio). We characterize the energy per successful transferred byte for radio \( i \) as

\[
E_{\text{byte},i}(d) = \frac{E_{\text{tx},i}}{B_{\text{rx},i}(d)},
\]

where \( E_{\text{tx},i} \) is the total amount of energy spent in transmitting data and \( B_{\text{rx},i}(d) \) is the number of received bytes for distance \( d \in [0, d_{\text{max}}) \). Generalizing [18, Sec. III-A] we define

\[
B_{\text{rx},i}(d) = \frac{L}{L + H} [1 - \text{erfc}(f_i(d))]^{L+H},
\]

where \( L \) and \( H \) are the payload size in bits and the amount of overhead in bits, respectively, and \( \text{erfc}(.) \) is the complementary error function. We define the signal quality decay function

\[
f_i(d) = \left( \frac{d}{a_i} \right)^{-r_i},
\]

\( a_i \) as radio-intrinsic correction value and \( r_i \) as loss coefficient. For example, a typical value of \( r_i = 2 \) for active radio or \( r_i = 4 \) for backscatter radio. Now, based on the above model we pose the following lemma:

**Lemma 1.** Any hybrid radio composed of \( n \) platforms has limited range after which the energy consumption per byte goes to infinity.

**Proof.** \( \forall n \lim_{d \to +\infty} B_{\text{rx},i}(d) \to 0 \Rightarrow E_{\text{byte},i} = E_{\text{tx},i}/B_{\text{rx},i}(d) \to +\infty \) which completes the proof.
Lemma 1 leads to the following corollaries:

**Corollary 1.** Defining $E(d) \triangleq \{E\text{byte},1(d), \ldots , E\text{byte},n(d)\}$ if $\exists E\text{byte},i(d) \in E \forall E\text{byte},j(d), i \neq j [E\text{byte},j(d) < E\text{byte},i(d), \forall d]$ then radio $i$ can be excluded while designing a hybrid radio.

**Corollary 2.** The maximum range of a system is limited by the radio with the largest range.

**Corollary 3.** At distance $d$ the hybrid radio energy consumption per byte is limited by the radio with the lowest energy consumption.

### 2.4 Measurement

To verify this simple analytical model we need to measure the consumed power of each radio as a function of the signal loss. We first introduce the selected hardware for BLE, WISP and finally the measurement setup.

#### 2.4.1 Bluetooth Low Energy—Transmitter/Receiver

We selected Nordic Semiconductor PCA10005 evaluation module (shown in Fig. 2.1) with an NRF51822 BLE System on Chip (SoC) [19] as BLE transmitter. The software used on the BLE radio is a customized firmware version (source code is available via [20]) transmitting only standard advertising messages [10] at a constant rate of 120 Byte/s. BLE has a maximum packet size smaller than the selected payload (i.e. 24 Byte) therefore each transmission consists of multiple packets. A second identical NRF51822 module is used as BLE receiver—continuously logging advertisement messages originating from the BLE transmitter. The BLE transmitter is configured to transmit advertisement messages with a length of 36 Byte (see Appendix B.2.2).

![Figure 2.1: The Nordic PCA10005 [19] development module.](image)
2.4.2 Computational RFID—Transmitter/Receiver

We select WISP 5 as a state of the art CRFID platform [6], see Fig. 2.2. The WISP 5 used for experiments has the RF energy harvester disabled by desoldering the output pin of the buck converter. This modification simplifies the energy measurement, as the energy provided to WISP 5 is not fluctuating in time as in the case of harvested energy. The WISP 5 firmware is adapted (see again [20]) to transmit with the same data rate as BLE. Again, as in the case of BLE, since the maximum payload of WISP 5, i.e. 12 Byte, is smaller than 120 Byte each message consists of multiple packets. The RFID receiver used is an Impinj Speedway R420 [21] (firmware version 4.8.3.240) controlled via the SLLURP Low-Level Reader Protocol (LLRP) library [22] connected to a Laird antenna [23].

Based on observations by [24, Sec. 4.1] we have chosen to use the EPC C1G2 Electronic Product Code (EPC) field as our data carrier instead of the Read command. Using the EPC field cuts down on the protocol overhead because it halves the amount of roundtrips [14, Sec. 6.3.2.12.3]. According to [14, Sec. 6.3.2.1.2.2] the length of the EPC field may be set between zero and thirty one words. For our experiments we set the EPC length to 12 Byte, in combination with the Query command, RN16 replies and Acknowledgement (ACK) messages this comes down to 23 Bytes (see Appendix B.2.3). While it is possible to let the WISP transmit longer EPC values to reduce the overhead even more, it also increases the probability of an error corrupting the message [18].

2.4.3 Measurement Setup

We measure energy per byte at the receiver (separately for BLE and WISP) as a function of signal attenuation. This is realized with two signal attenuators [25] connected in series. The attenuation range of this attenuation chain is 0 dBm to 149 dBm, which is larger than the maximum sensitivity of both receivers. These attenuators limits the signals bi-directionally and therefore both uplink and downlink are attenuated at the same time.

\footnote{Please note that this ACK message acknowledges the handshake and \textit{not} the data transmission}
Both BLE transmit/receive evaluation boards are equipped with antenna connectors allowing to connect attenuators directly. WISP, on the other hand, does not provide such an antenna connector and therefore it is positioned at a fixed distance of 50 cm from the interrogator antenna which is then connected to the RFID interrogator via the attenuators. In the results we correct the WISP measurement by adding the theoretical loss for 50 cm at 900 MHz which is 
\[ 20 \log 4\pi \left( \frac{x}{\lambda} \right) = 20 \log 4\pi \left( \frac{0.5}{0.33} \right) \approx 25.6 \text{dB} \, . \]

The BLE module [19] has an uncalibrated approximate transmission power setting accessible via the Application Programable Interface (API) of the S110 softdevice. In experiment we tested highest (4 dB) and lowest (–30 dB) possible transmission power. The RFID-reader has been tested for the maximum transmission power of 32.5 dB.

We measure the power consumption of both radios using a self developed, buffered, differential, sensing circuit monitoring the voltage drop over a 100Ω shunt resistor in series with the Device Under Test (DUT). This circuit is coupled to a Tektronix MDO4054B–3 [26] oscilloscope to measure power consumption over time which is used to calculate the energy consumption. Schematics of this measurement device are available via [20].

### 2.4.4 Measurement Results

The relationship between energy per byte and distance, as measured for both active and backscatter radio and complementary fitted plots, is shown in Fig. 2.3. As expected, the WISP—while more energy efficient in good channel conditions—also has a shorter range of operation compared to the active BLE radio. Based on the system requirements a short range might be a desired feature, but in this project we see it as a undesired side-effect. A notable feature of the results is their shape. Instead of a gradual increase in energy consumption per received byte, as one point the energy per byte metric starts to rapidly increase for both platforms. This “brick wall” effect [18, Sec. V] is caused by the increasing amount of bits failing to correctly reach the receiver, which at one point becomes too large, which causes the whole packet to be lost.
Figure 2.3: **Power per byte over distance for WISP and BLE.** Note that what seems to be an energy efficient radio in one range might be an energy inefficient radio in another range. The dashed data points are extrapolated, the constant power consumption for the BLE radio and all data being received, yields constant energy per byte. Fitted plots are based upon (2.2). Parameters for a fitted WISP curve: $a_i = 60$, $d_i = 4$, $E_{tx,i} = (L + H)5\mu J$ with $L$ and $H$ as in Section 2.4.2. Parameters for a fitted BLE curve: $a_i = 85$, $d_i = 2$, $E_{tx,i} = (L + H)21\mu J$, $L$ and $H$ as in Section 2.4.1.
2.5 Solution: Multi-Radio Systems

Following the results shown in Section 2.4.4 we propose a hybrid multi-radio solution. A combination of backscatter radio and active radio seems to be the logical step to solve the imperfections of both systems. Unfortunately, to the best of our knowledge, no such complete implementation exists which calls for immediate investigation of such hybrid platform. One obvious way of using BLE to extend the RFID range is to use multiple RFID readers which are coupled using BLE, as proposed for different radio types (with node-to-node communication) by [27]. Unfortunately, this approach cannot be followed here because state of the art CRFIDs cannot communicate with other CRFIDs without the RFID-reader. The only hybrid active/backscatter platform we are aware of is [28], which uses BLE to reprogram a backscatter testbed, and does not use BLE for improving backscatter reliability.

Authors of [29] propose a method of using BLE as a physical transport layer for an RFID protocol. A backscatter-BLE receiver is proposed in [30], which can be used to receive backscatter communication. In the non-backscatter context an approach to combine multiple heterogeneous radios by [31] uses the acknowledgement delay and machine learning mechanisms to optimize system performance.

All above mentioned multi-radio platforms rely on acknowledgements from the receiving party and/or active radio transmissions. Unfortunately such acknowledgment mechanism does not exist in EPC C1G2 protocol, which makes design of BLISP challenging.

2.6 Alternative Solutions

The question remains, whether in the light of this observation hybrid radio platform is the only solution to improve energy efficiency and transmission range of CRFID. In this section we review some of the alternatives.

2.6.1 Low Power Active Radio with Battery

The simplest alternative to the hybrid platform would be a connection of a sufficiently large battery and BLE radio.

**Limitation:** Unfortunately, all batteries will eventually deplete leading to expensive battery (or even the whole device) replacement. For battery replacement the device must be physically accessible, as it is impossible to wirelessly restore the energy level of the battery without an harvester.
2.6.2 Power Harvester with Active Radio

Wireless RF power harvesters solve the physical accessibility and battery constraint.

**Limitation:** Inefficiencies in RF power harvesters, energy storage, energy conversion, and energy transmission through RF waves, cause that no power harvester and active radio combination will be as energy efficient as a backscatter radio.

2.6.3 Backscatter Radio with Improved Channel Coding

The operational reliability and robustness of communication of CRFIDs could be improved by adding a more extensive channel coding mechanism. For example: WISP is currently limited to the FM0 coding [14, Sec. 6.3.1.3.2.1], in which each bit is represented by one signal alternation for each symbol. Miller coding methods [14, Sec. 6.3.1.3.2.3] have more alternations for each symbol, reducing the possibility of bit-flips harming the messages.

**Limitation:** Channel coding would indeed make CRFID more robust (i.e. would shift the WISP curve to the right in Fig. 2.3), but would still keep CRFID susceptible to reflections and destructive interference. Finally, we conjecture, this would still not make WISP at least as energy efficient as BLE in the broad attenuation range.

2.6.4 Improved Energy Harvesting for CRFID

Considering literature related to energy storage in CRFID, we need to mention [17] proposing to store unused energy in battery/capacitor for future use and [32] where energy storage from wireless signals has also been proposed in combination with Wi-Fi communication.

The ability to harvest power from the environment mitigates the need for on-device energy storage facilities like batteries. The absence of batteries directly removes the need for expansive and expensive battery replacement.

**Limitation:** The addition of long term power storage would most certainly increase the maximum range in which CRFID will be able function. However, it will do so by limiting the duty cycle in which the system is able to transfer data. Moreover there is the inevitable failure for long-term out of range situations. As with additional channel coding (see Section 2.6.3), this solution only shift the problem into a new range.
Chapter 3

BLISP: Architecture and Implementation

We are now ready to introduce BLISP, our hybrid backscatter and active radio platform, to help exploit the main trade-offs as proposed in Lemma 1 and Corollaries 1 to 3. The BLISP infrastructure mainly consists of two parts: (i) a COTS RFID interrogator combined with a BLE receiver; and (ii) a multi-radio sensor node—the BLISP. To provide a flexible platform we opt to combine two readily available radio platforms instead of developing our own (integrated into a single silicon) platform.

A complete system level overview of the BLISP is shown in Fig. 3.1. The main design principle behind BLISP is the absence of any algorithm on the receiver side, the receiver only merges the multiple data streams received by the different radios.

First, in Section 3.1 the BLISP hardware design will be presented. Section 3.2 introduces the BLISP software architecture. Section 3.3 will explain why standard channel estimation methods are not suitable for BLISP, and proposes a new feedback-less method. Finally, Section 3.4 introduces two radio switching methods based on the aforementioned estimation algorithm.

3.1 BLISP Hardware Architecture

The chosen radio modules for this platform are the same as described in Section 2.4. A Printed Circuit Board (PCB) has been designed to ease the connection of the two separate radio platforms, see Fig. 3.2. The PCB connects the active and passive radio, and provides means for radio collaboration and energy distribution.
Figure 3.1: **Overview of the BLISP system consisting of one transmitter and one receiver.** The temperature sensor providing data is part of a WISP but displayed separately for clarity and completeness. All displayed connections depict a flow of energy or data and do not directly correspond to physical connections. For a detailed description of the physical connections see [20]. †For the mobile reader experiments the Impinj R420 is replaced by a MTI MINI ME, while the NRF51822 is replaced by the internal BLE receiver of a Samsung Galaxy S3, see Section 3.1.3. ‡The BLISP should be able to store harvested energy (not implemented).
(a) The top side of the BLISP with annotations for the most important components. Please note that the WISP antenna is not fully shown.

(b) Bottom side of the BLISP. Symbolically illustrated directional connections by color, as numbered: (1) white: ground; (2) brown: clear to send; (3) red: BLE power supply; (4) green: WISP to BLE serial channel; (5) orange: BLE to WISP serial channel (unused); (6) yellow: ready to send, and (7) blue: WISP power supply.

Figure 3.2: The BLISP PCB as seen from top (Fig. 3.2(a)) and bottom (Fig. 3.2(b)). PCB design available via [20].
As active radio component for the BLISP we use the same NRF51822 BLE module as described and evaluated in Section 2.4.1. As backscatter radio we use the same WISP 5 platform as described and evaluated in Section 2.4.2.

### 3.1.1 Radio Collaboration

To ensure continuous communication while switching between radios, a communication channel is needed to convey desired state information for the active radio and to share sensor values between the two separate radios.

The NRF51822 BLE module has a silicon bug causing high power consumption by perpetually keeping non-vital microcontroller peripherals enabled [33, Id 39]. This bug unfortunately affects all conventional (digital) communication channels and General Purpose Input/Output (GPIO)-interrupts, rendering them useless as low power wake-from-sleep devices. The low power analog comparator peripheral is not affected by this bug. Therefore this peripheral is used as wake-up signal for the higher throughput Universal Asynchronous Receiver/Transmitter (UART) acting as flow control. The analog input is monitored for rising and falling signal levels and enables and disables the UART accordingly. The BLE radio also uses a digital output as CTS to signal the current UART state back to the WISP.

The message format as used for the UART communication can be found in Appendix B.2.1.

### 3.1.2 Energy Harvester

WISP is not only backscatter radio but also power harvester. To be able to use the harvested energy to power the BLE module we need to store energy. For this an ultra-low-power all-in-one boost converter, battery charger and buck converter chip [34] is used. Adding this chip enables the system to store more energy and therefore do more calculations or active transmissions. The charger also enables the device to work on larger distances with a low duty cycle as shown by [17].

### 3.1.3 BLISP Receiver/Sink

The receiving side of BLISP consists of two receiving radios matching the two transmitting radios. The BLISP receiver is as simple as possible and only merges the data streams from the receiving radios. Because the receiver does not make any decisions about which radio to use, the BLISP can switch without synchronisation mechanisms in conjecture to [31].
We present two different reader setups: (i) a fixed computer-centered; and (ii) a mobile smart phone-centered setup.

### Fixed Receiver

The fixed receiver consists of a host computer with an ethernet connected Impinj Speedway R420 [21] and a by serial interface connected Nordic Semiconductor NRF51822 [19]. This setup is the same as given in Section 2.4.2.

### Mobile Receiver

In this section we show the applicability of the BLISP in less favorable situations, e.g. with a less powerful RFID-reader. The mobile receiver setup consists of a smartphone with build-in BLE radio combined with an external COTS mobile RFID-reader. The MTI MINI ME [35] supports the same EPC C1G2 protocol as WISP and is connected to the smartphone via the micro-USB port. Based on the API provided by MTI we log all EPC C1G2 inventory data\(^1\).

Unfortunately, when used unmodified, the MINI ME can only inventory WISP (with fixed power supply) up to a maximum range of 2 cm. Therefore, to increase the inventory range of MINI ME, we replaced the embedded antenna with a 2 dBi GSM band omnidirectional one [37]. By replacing the antenna, the maximum inventory range was extended to 10 cm. Table 3.1 shows a parametric comparison for the two reader platforms, while Fig. 3.3 shows the MINI ME reader with GSM antenna connected to a smartphone running our measurement application.

\(^1\)Smartphone software developed by Qingzhi Liu and based on [36], available at [20]
3.2 BLISP Software Architecture

The WISP component of the BLISP software consists of 1674 lines of C code and 1847 lines of assembly code. Around 1000 lines C and 500 lines assembly were written in the BLISP development process of which around 600 lines C and 50 lines assembly are BLISP specific. The remaining part is based upon [39]. The BLE element consists of a BLISP specific 500 line C program and the NRF51822’s API. The fixed BLISP host currently consists of various Bash and Octave scripts with varying lengths. The mobile host consists of 750 lines of customized Java code.

3.2.1 Wireless Identification and Sensing Platform

Because of the low power requirements and therefore our preference for backscatter communication we choose to have a WISP acting as master over a BLE radio. Between the periodic sensing and transmission rounds a WISP is put into a low power sleeping state.

For all following experiments WISP measures temperature and a timestamp since the startup\(^2\). The timestamp is included for evaluation purposes, as this value enables to evaluate the number of missing and/or duplicate packets. To ensure a constant data stream in case of radio switching the sensor data is periodically shared with the BLE radio as described in Section 3.1.1.

\(^2\)Other possible sensors are the accelerometer, already available on a WISP, or any other (low power) electronic sensor.
The BLE radio and the a WISP are both set to have 12 Byte payload per message and ten messages are combined into a single transmission. As the temperature data combined with the timestamp only uses 4 Byte the message is padded with 8 Byte constant data in the form of 0x001122···nn.

Because of incompatibilities between a WISP and the MINI ME RFID reader used for the mobile host experiments the EPC C1G2 tag select mechanism [14, Sec. 6.3.2.3] is disabled for all fixed and mobile reader experiments. When used, the tag select mechanism limits the number of tags replying to Query commands by dividing them in subsets based on user-defined criteria.

3.2.2 Bluetooth Low Energy

A BLE module (as decribed in Section 2.4.1) is programmed as slave under a WISP. As described in Section 3.1.1 the BLE radio is periodically awaken by the WISP to receive new data. When not wirelessly transmitting nor receiving data from a WISP a BLE module is put into a low power state.

3.3 Backscatter Channel Estimation

The estimation of the upstream backscatter channel quality is not trivial. We propose a method of estimating the backscatter channel and use this estimation to select backscatter or an active radio on-the-fly. We start with reviewing classical solutions.

3.3.1 Classical Estimation Methods

Because backscatter radios behave differently than active ones, typical channel estimation methods do not directly apply.

EPC C1G2 Protocol Feedback

The de facto standard method of assessing packet reception rate is to query the receiving party if it indeed received a packet. For most protocols this quality assurance is done by acknowledging (all) received packets.

**Limitation:** The default method of awaiting an ACK message for each transmitted data message is not possible. Within the EPC C1G2 [14] protocol there are no standard facilities to guarantee the successful reception of a EPC values transmitted by a tag. The exclusion of this functionality is logical for standard RFID tags, as they are computationally limited, transmit an mostly
unchanging identifier, and most likely could not handle retransmissions. Transmitting data back to a CRFID also implies that a CRFID should handle computationally hard, and a protocol-wise large overhead inducing write accesses.

**BLE Protocol Feedback**

The more responsive BLE channel could be used to provide a feedback channel for the reception of RFID packets transmitted by a CRFID.

**Limitation:** The introduction of a separate radio channel could increase reliability because the channels might break down under different circumstances. It might also decrease reliability because the BLE channel might be broken while the RFID channel is in working order. Practically, including a BLE radio in receiving mode will also dramatically decrease the energy efficiency of a platform, as the radio has to listen for an extended (worst case: continuous) period of time.

**RSSI Strength Feedback**

Neither a CRFID hardware nor a EPC C1G2 protocol has a built-in support for Received Signal Strength Indication (RSSI) measurement on the RFID transmission. A coarse method to estimate the vicinity of a RFID reader is by measuring the amount of energy harvested by the CRFID. If a tag is close to a reader, it is easily possible to harvest energy, while if a tag is far away it would be almost impossible to harvest it. The BLE radio has native support for RSSI measurements on the received messages.

**Limitation:** Measuring RSSI for the signal originating from the RFID-reader and received by the backscatter radio does not directly correlate with the channel quality for backscatter data (as there is no constructive interference as explained in Section 1.1). While the interrogator knows the RSSI, the backscatter device cannot reliably determine it. An BLISP could also query the RFID reader for its own RSSI as measured by the reader, this would induce relatively a lot of overhead on both the reader and CRFID side.

In order to retrieve RSSI values from the BLE it should be placed into listening mode, which is more power consuming than the transmission mode. Enabling the BLE radio only for channel estimation without using it for data transfer is a loss of energy.
3.3.2 Proposed Estimation Method

For the BLISP system we propose a novel, less standard way of estimating the channel. If an RFID interrogator and tag perform a multipart handshake, the backscatter channel is usable to transfer data.

Work of [5] proposed an approach for setting an interrogator to its optimal settings based on both measured RSSI and packet loss. Contrary, our system does these, packet loss-based, estimations on the sensor side instead of at the interrogator.

While the EPC C1G2 protocol does not include a data acknowledgement mechanism it has a bidirectional handshake before the data exchange. See Fig. 3.4 for an overview of the handshake (points 1 to 4) and EPC data exchange (points 4 and 5). Part of this handshake is the tag sending the reader a random number (RN16, point 2), which the reader should acknowledge if received correctly by an ACK message (point 3) containing this random number. If the tag correctly receives this ACK message (point 3) containing the same random number it just transmitted, it has knowledge about the backscatter channel quality.

If the message would have got corrupted, either from the tag to the reader or from the reader to the tag, the received ACK message would not be correct or not contain the correct RN16. To reach the ACK message both channels (to and from) the CRFID tag need to be in a state good enough to also transmit payload data (point 4).

By measuring the number of successful handshakes and comparing this number to the amount of packets we expected to transmit, we estimate the quality of the RFID communication channel. The RFID-reader tries to maintain an as fast as possible rate, therefore if no ACK was received we can be sure that there is no reader within the communication range.

Figure 3.4: **Simplified example of tag inventory EPC C1G2.** Note that there is no acknowledgement to signify data reception. See [14, Annex E] for further reference.
Algorithm 1 BLISP Control Protocol

1: $x \leftarrow$ Maximum backoff window, see Section 3.4.1
2: each Period do
3: \hspace{1em} $a \leftarrow \#\text{ACK}_{n-1}$ \hspace{1em} \triangleright \text{Received ACKs}
4: \hspace{1em} $r \leftarrow \#\text{FRAME}_{n-1}$ \hspace{1em} \triangleright \text{Frames planned to transmit}
5: \hspace{1em} WISP\text{\_ok} $\leftarrow (a = r)$ \hspace{1em} \triangleright \text{Expect ACK for each frame}
6: if WISP\text{\_ok} then
7: \hspace{1em} Backoff $\leftarrow 0$ \hspace{1em} \triangleright \text{No backoff on success}
8: end if
9: if 0 = Backoff then
10: \hspace{1em} WISPTX $\leftarrow$ true \hspace{1em} \triangleright \text{Is (re)try slot?}
11: \hspace{1em} if \neg WISP\text{\_ok} then
12: \hspace{1em} \hspace{1em} Backoff $\leftarrow l(0,x)$ \hspace{1em} \triangleright \text{New uniformly random backoff}
13: \hspace{1em} end if
14: else
15: \hspace{1em} WISPTX $\leftarrow$ false
16: \hspace{1em} Backoff $\leftarrow$ Backoff $-1$ \hspace{1em} \triangleright \text{Shift backoff}
17: end if
18: BLETX $\leftarrow$ \neg WISP\text{\_ok} \hspace{1em} \triangleright \text{Use BLE if not use WISP}
19: end each

3.4 Radio Switching

As briefly addressed in Section 1.1 backscatter is more sensitive to interference and reflections than most active radio standards. The circumstances and environmental influences affecting the performance of the WISP are likely to change in an irregular and unpredictable way.

3.4.1 Random ($< x$)

We propose that making the switching mechanism dependent on the past will decrease the number of unnecessary backscatter channel evaluations, thereby reduce overhead and improve energy efficiency. Because we assume the environment to act random and unpredictable we opt that it does not make sense to include a sophisticated self-learning algorithm. Our random backoff approach implements an ALOHA-inspired random backoff window with maximum value $x$.

A low value of $x$ will make the system more responsive while a high value will make the system more stable in the long run. A pseudo-code representation of this algorithm in shown in Algorithm 1, which shows that the algorithm only depends on results of the previous transmission.

3.4.2 Naïve

Limiting the maximum random value to zero will generate a constant as-short-as-possible backoff window resulting in the naïve approach. This approach (used as a baseline reference) assures that we use WISP as much as possible which increases energy efficiency. At the same time, checking a perpetually broken WISP communication channel induces an overhead compared to other maximum backoff window sizes.

\[\text{The method of generating random numbers is described in Appendix B.1}\]
Chapter 4

BLISP: Experimental Evaluation

To test the performance of BLISP we have executed several experiments measuring both goodput and energy consumption.

First, Section 4.1 introduces how the experiments were performed with replicability as an important feature. Section 4.2 will show the BLISP to be as robust as BLE and thereby more robust than WISP. This section also shows the BLISP to consume less power than BLE for most situations, while only slightly increasing power consumption compared to WISP. Finally, Section 4.3 shows that the BLISP also improves overall performance when used in combination with a smartphone attached RFID-reader.

4.1 Experiment Setup

Our experimental setup consists of hardware components and methodologies for replicable and traceable measurements. For this test the BLISP as described in Chapter 3 is considered.

The measurement and evaluation setup we use for these experiments is based on the setup described in Section 2.4.3. In addition we use an automatic three-dimensional positioning crane [38] situated in a lab environment to automate the experiments involving a mobile BLISP.

4.1.1 Measurement Replicability

According to Fig. 2.3 wireless radios have two main ranges of operation, within the first range most of the packets get received and therefore the
energy per byte ratio stays rather constant, within the second range almost no packets are received and the energy spend on transmitting a byte therefore increases drastically.

For the BLISP performance tests we limit the transmission power and sensitivity of a RFID reader and define two static positions based on a WISP communication abilities, one in WISP-range and one outside WISP-range. The experiments were performed by placing the BLISP in the in-range spot, placing the BLISP in the out-range spot, and alternating the BLISP location between the in- and out-range positions on a predefined constant time interval (10 s) to simulate an uniformly distributed mobile application. The BLE radio was in range for all experiments, otherwise the system would fail according to Corollary 2. The time duration for each experiment was 2 min and each experiment was repeated five times.

We run baseline experiments for a battery powered WISP and a BLE radio transmitting at 4 dBm as used in Chapter 2.

4.1.2 Data Acquisition

During these measurements we log the number of received packets for both the RFID and BLE receivers. The power consumption measurements are made by using the programmer interface to supply power using the EnergyTrace platform [40] integrated in the programmer and Integrated Development Environment (IDE).

To perform the measurements in a repeatable way we created a script handling repetitions, timing and synchronization between multiple platforms involved in our setup. Due to non-consistent startup delays within the involved platforms, we match the start and stop of our experiments by asynchronously starting all platforms and logging the state of all platforms after a predefined empirically found startup delay of 3 s which is longer than the startup time of the slowest component. Other solutions to this synchronisation problem would be to reverse-engineer the EnergyTrace protocol or use an entirely other platform. Using an other platform would be unfavorable because the EnergyTrace device is also used as WISP programming interface to reset the WISP to its default state after each experiment.

This process is repeated for the stop moment after which all platforms asynchronously get stopped and reset to their default states.

Because of the limited API for the EnergyTrace platform we use synchronously timed screen shots and Optical Character Recognition (OCR) to log the energy measurements for experiments in which the EnergyTrace is used.
4.2 Static RFID Reader Experiment

Results of the experiments are shown in Fig. 4.1, showing both transferred data, see Fig. 4.1(b), and efficiency in energy per byte, see Fig. 4.1(a). Due to normalization to unique messages, the energy per byte values in Fig. 4.1(a) are around ten larger than the numbers presented in Fig. 2.3.

Our experiments show that BLISP increases goodput almost instantly in the long range compared to a normal WISP (see Lemma 1) while not severely increasing power consumption over a WISP in the short range. On the other hand BLISP almost halves energy consumption in the short range compared to a normal BLE radio while only slightly increasing energy consumption by 10% on the long range. As we add a mobility factor to the experiment we see WISP loosing a share of messages corresponding to the relative out of range time, this increases the energy per byte metric to the same level as the active BLE radio which is able to transfer data in all positions. The combined system cannot do a better job at energy efficiency than the lowest energy consuming radio for a certain position (as stated in Corollary 3).

When applied to an uniformly distributed in-/out-range mobility pattern, the energy profit in short range is nullified by the energy cost in the long range. For only out of range situations the BLISP is not a good solution, as also mentioned in Corollary 1. BLISP improves energy efficiency and throughput for situations in which the WISP can be used for at half of the time.
Figure 4.1: Results of the WISP, BLE and BLISP evaluation using Impinj R420 RFID-reader. Because the WISP is not able to transmit data over a long range, see Fig. 4.1(b). The WISP is effectively wasting all energy, hence the energy per byte metric is infinite for this measurement, see Fig. 4.1(a). Contrary to WISP, BLISP ensures a constant goodput in all situations. Corollary 3 holds for all situations, i.e. in the short range BLISP cannot be more energy efficient than WISP, while in the long range BLISP consumes more energy than BLE. We show the only WISP, only BLE, naïve BLISP and random ($< x$) BLISP for $x \in \{3, 10\}$. These experiments have been normalized to uniquely received messages to eliminate messages transmitted by both radios at switching moments.
4.3 Mobile RFID Reader Experiment

The experiment setup parameters on the BLISP side is the same as using fixed RFID reader in Section 4.1. The detail setup parameters of mobile data aggregator are as in Table 3.1.

Results for the mobile host experiments as shown in Fig. 4.2 show comparable results among WISP, BLE and BLISP compared with fixed reader experiments from Section 4.2. The relative improvement from BLE to WISP and naïve-BLISP using a mobile reader is even larger while in-range. This relative improvement is most likely to be caused by the smartphone’s BLE module to be worse than the NRF51822 receiver.

Interestingly, for in-range measurements, a large backoff window shows worse performance than the naïve and small backoff experiments. We suspect that this is caused by the hardware limitation of MINI ME. Based on experiments, the MINI ME reader has trouble with rapid changing or only shortly available RFID tags. Fortunately, the BLISP algorithm detects the failing RFID reader and correctly enables the BLE radio which results in continuous data availability.
Figure 4.2: Results of the WISP, BLE and BLISP evaluation using MiniMe RFID-reader. In the long range the MINI ME reader is not able to receive data transmitted by the WISP, see Fig. 4.2(b), therefore the energy per byte is infinite, see Fig. 4.2(a). For this experiment we only measured the static in range and out of range locations. Because of limited logging capabilities on the smart phone the number of messages is not normalized to unique messages.
Chapter 5

Summary

We conclude the thesis by summarizing limitations in Section 5.1, presenting possibilities for future work in Section 5.2. Finally, we conclude with our conclusions in Section 5.3.

5.1 Limitations

Our multi-radio BLISP system is limited in energy performance. As stated in Corollary 3, it is impossible to consume less energy than the most efficient radio for a certain situation, e.g. we cannot consume less energy than WISP on the short range, and we will consume at least as much energy per byte as BLE in long range.

5.2 Future Work

We list the most important limitations and action items for future work:

1. **Switching mechanism requires further research**: As long as the BLISP spends the majority of its runtime in the short (WISP-capable) range using our proposed system yields profit.

2. **Micro-controller overhead**: The current BLISP is build using two separate radio modules and therefore also has two micro-controllers. It is preferable to use one micro-controller to reduce energy consumption.

3. **Limited to two radio platforms**: By Corollary 2 and Corollary 3 adding different kinds of radios will increase the performance of BLISP.
4. **Limited performance of energy harvester:** Add more efficient (multi-frequency) power harvester.

5. **Limited link layer:** Enhance backscatter radio range/applicability by using dynamic message length or other channel coding.

### 5.3 Conclusions

In this thesis we design, implement, and evaluate a platform combined of BLE and WISP which we call BLISP. In experiments this heterogeneous hybrid radio platform shows that for situations in which most of the time is spent within the comfort region of the lowest power radio, the energy efficient is improved compared to the higher power radio while at the same time the reliability of the system is larger than the reliability of the lower power radio. We also demonstrate that it is possible to have this heterogeneous radio platform operating in a perennial way with the addition of a wirelessly rechargeable energy storage device. Lastly we show that the combination of these two different wireless radio paradigms supports our theoretical expectations.
Appendix A

BLISP PCB

(a) Annotated picture of BLISP top side

(b) PCB design for BLISP top side

Figure A.1: The top side of the BLISP
(a) Annotated picture of BLISP bottom side. Symbolically illustrated directional connections by color, as numbered: (1) white: ground; (2) brown: clear to send; (3) red: BLE power supply; (4) green: WISP to BLE serial channel; (5) orange: BLE to WISP serial channel (unused); (6) yellow: ready to send, and (7) blue: WISP power supply.

(b) PCB design for BLISP bottom side

Figure A.2: The bottom side of the BLISP
Appendix B

BLISP Firmware

B.1 Random Number Generation

The random number generator used for the random backoff (see: Section 3.4.1) in the WISP is really a deterministic pseudo-random number generator. The process of generating random numbers consists of the following steps:

B.1.1 Offline–Random Data Generation

The run-once program from the WISP 5 repository is being run before running any real application to generate an in (Ferroelectric Random Access Memory (FRAM)) memory table of random values. Because of the noisy nature of Analog to Digital Converters (ADCs), the Least Significant Bit (LSB) from ADC readings has a random-like value, which results in a random bitstream.

B.1.2 Online–Random Number Generator

At runtime, when a random number is needed, the program gets value $x$ with index $i$ from the list with random numbers and increases $i = i + 1$. The value of $x$ is then put through function $f(x) = (x\&3_8) + (x\&31_8)$ to get a better uniformly distributed random number. Finally the random number is limited to the desired maximum value by using a modulo operation: $r = f(x) \mod y$ with $r$ being the random number, $x$ the bitmasked list value and $y$ the maximum random value.
B.2 Message Formats

As a communication system, the BLISP system we propose has multiple messages. Bitfields for WISP to BLE communication (see Appendix B.2.1), RFID handshake and EPC exchange (see Appendix B.2.3), and BLE advertisement (see Appendix B.2.2) are described.

B.2.1 WISP to BLE

To ensure a continuous data stream while switching radios, the WISP shares sensor data with the BLE module. **Note:** The state control byte could be replaced by a bit to save on data, a byte is used for easy debugging and is not limiting the system.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>7</th>
<th>8</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BLE Switch</td>
<td>Time Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>23</td>
<td>24</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Time Sensor</td>
<td>Thermal Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>39</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thermal Sensor</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **BLE Switch** Use Bluetooth Low Energy? U for enable, D for disable;
- **Time Sensor** Time in seconds since WISP reset;
- **Thermal Sensor** Temperature as measured by WISP.
B.2.2 BLE Advertising

Advertisement messages are broadcasted on special channels and do not include handshake or feedback. A advertisement message with 12 Byte payload is shown.

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>8</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>23</td>
<td>24</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>39</td>
<td>40</td>
<td>43</td>
</tr>
<tr>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
</tr>
<tr>
<td>48</td>
<td>53</td>
<td>54</td>
<td>55</td>
</tr>
<tr>
<td>56</td>
<td>57</td>
<td>...</td>
<td>144</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>148</td>
</tr>
<tr>
<td>150</td>
<td>151</td>
<td>152</td>
<td>159</td>
</tr>
<tr>
<td>160</td>
<td>167</td>
<td>168</td>
<td>175</td>
</tr>
</tbody>
</table>

**Preamble** Internal protocol management. 101010102 for advertising;

**Address** Access address. 8E89BED68 for advertising;

**Type** Message type. 00102 for *non connectable undirected advertising*;

**TxAdd** Address is public when 0, random otherwise;

**RxAdd** *Not used by non connectable undirected advertising*;

**Length** Payload length in Bytes;

**Payload** Advertised data;

**CRC** Message checksum.
B.2.3 WISP to Host

The WISP to host/reader communication makes use of the EPCglobal Class 1 Generation 2 (EPC C1G2) protocol, we list the important messages.

**Query Command (R→T)**

Each handshake starts with the reader broadcasting a Query command, containing connection parameters, to which tags might reply [14, Fig. 6.21].

<table>
<thead>
<tr>
<th>Command</th>
<th>DR</th>
<th>M</th>
<th>TR</th>
<th>Sel</th>
<th>Session</th>
<th>Target</th>
<th>Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q</td>
<td>CRC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Command**: EPC C1G2 command. 1000₂ for Query;
- **DR**: T→R link frequency;
- **M**: Cycles per symbol. Data rate and modulation format;
- **TR**: Enable pilot tone before preamble;
- **Sel**: Chooses which tags respond. *Unused*;
- **Session**: Session for the inventory round. 2 for WISP;
- **Target**: Include already inventoried tags. *Unused*;
- **Q**: Number of slots in round equals 2⁰;
- **CRC**: Message checksum.

**RN16 Reply (T→R)**

The RFID tag, if allowed, replies a sixteen bit pseudo random RN16 value.

<table>
<thead>
<tr>
<th>RN16</th>
</tr>
</thead>
</table>

- **RN16**: 16bit random number used to further identify tag.
**ACK Command** (R→T)

The reader acknowledges the tag with Acknowledgement (ACK) message.

<table>
<thead>
<tr>
<th>Command</th>
<th>RN16</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 7 8 15</td>
<td></td>
</tr>
</tbody>
</table>

**EPC Reply** (T→R)

Finally, when the correct ACK has been received the tag replies with its identifier. In the case of our BLISP this identifier contains payload.

<table>
<thead>
<tr>
<th>Stored PC</th>
<th>EPC</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 7 8 15</td>
<td>103 104 105 106 107</td>
<td>108 115 116 123</td>
</tr>
</tbody>
</table>

**Stored PC** Protocol-control field. Contains tag capabilities. Contains EPC-length, user-memory indicator (UMI), XPC_W1 indicator (XI) and number system identifier toggle (T);

**EPC** Electronic Product Code. 92bit value for BLISP;

**CRC** Message checksum.
Bibliography


43