Ultra-low-power Bluetooth Low Energy (BLE) compatible backscatter communication and energy harvesting for battery-free wearable devices

Joshua F. Ensworth

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2016

Reading Committee:

Matthew S. Reynolds, Chair

Shyam Gollakota

John Sahr

Program Authorized to Offer Degree:
UW Department of Electrical Engineering

University of Washington

Abstract

Ultra-low-power Bluetooth Low Energy (BLE) compatible backscatter communication and energy harvesting for battery-free wearable devices

Joshua F. Ensworth

Chair of the Supervisory Committee:
Associate Professor Matthew S. Reynolds
Electrical Engineering & Computer Science and Engineering

This thesis explores new wireless power and backscatter communication architectures for ultra-low-power wireless sensors and other devices such as wearables. We first present measurement, analysis and harvesting approaches for extracting energy from 2.4 GHz wireless communication signals, including an approach for powering a relatively high power sensor in burst mode at an input power level of -15 dBm. We present the first backscatter-based data uplink approach that achieves compatibility between backscatter devices and billions of completely unmodified standard wireless devices using the Bluetooth Low Energy standard. We show that this data uplink approach can communicate with BLE receivers with a radio communication efficiency of 28.4 pJ/bit. This is over 100x lower energy per bit than conventional BLE transmitters. One microcontroller based implementation consumes over 6x less power than the best commercially-available Bluetooth transmitters, and can leverage both modulated and unmodulated carriers to provide the backscatter uplink. This allows us to transform one BLE signal as a carrier source for another BLE-Backscatter signal.

We investigate the range of the BLE-Backscatter system in both bistatic and monostatic, full-duplex application scenarios. The range analysis considers the BLE

receiver sensitivity and performance in the presence of self-jamming interference from the external carrier source in the bistatic case. We also present a carrier cancellation architecture that reduces self-jamming in the monostatic case. We characterize the packet error rate and received signal strength in both cabled and over-the-air scenarios. Finally we present an ultra-low power superheterodyne receiver architecture that leverages an external carrier as the local oscillator, removing the need for on board (or on chip) generation of the local oscillator signal. The receiver uses a two-port mixer for simultaneous mixing and power harvesting of the external carrier and desired BLE signal.

This thesis shows a path toward the widespread adoption of backscatter communication in low-power wireless devices such as smart watches, fitness bands, biomedical sensors, etc. Other wireless devices, such as sensors for the Internet of Things (IoT) where power consumption is a crucial consideration could also benefit from the approaches presented.

Contents

List of Tables

List of Figures

List of Abbreviations and Symbols

AC	Alternating current
AM	Amplitude modulation
ASK	Amplitude-shift keying
BER	Bit Error Rate
BFSK	Binary frequency shift keying
BLE	Bluetooth Low Energy
Bluetooth SIG	Bluetooth special interest group
BPF	Band-pass filter
CDMA	Code division multiple access
CMOS	Complementary metal-oxide-semiconductor
CPU	Central processing unit
CRC	Cyclic redundancy check
CW	Continuous wave
DC	Direct current
DUT	Device under test
DTV	digital television
EIRP	Equivalent isotropically radiated power
EPC	Electronic product code
ETSI	European telecommunications standards institute
FCC	Federal communications commission

FET	Field effect transistor
FM	Frequency modulation
FSK	Frequency-shift keying
FTP	File transfer protocol
GPS	Global positioning system
GSM	Global system for mobile communications
HPF	High-pass filter
HUDs	Heads up displays
IC	Integrated Circuit
IF	Intermediate frequency
I2C	Inter-integrated circuit
IoT	Internet of things
JFET	Junction gate field-effect transistor
LFSR	Linear feedback shift register
LO	Local oscillator
LOS	Line of sight
LPF	Low-pass filter
LQ	Linear-quadratic
LSB	Lower sideband
LTE	Long-term evolution
LVCMOS	Low voltage complementary metal oxide semiconductor
Mbps	Megabits per second
MBS	Modulated backscatter
MPPT	Maximum power point tracking
NFC	Near field communication
OFDM	Orthogonal frequency division multiplexing

OTA	Over the air
PCB	Printed circuit board
PDU	Payload data unit
PER	Packet error rate
POWs	Power optimized waveforms
PSK	Phase-shift keying
PV	photovoltaic
QAM	Quadrature amplitude modulation
RBW	Resolution bandwidth
SIR	Signal to interference ratio
SNR	Signal to noise ratio
SMA	SubMiniature version A
SMU	source-measure unit
SPI	Serial peripheral interface
RF	Radio Frequency
RFID	Radio frequency identification
UHF	Ultra high frequency
USB	Universal serial bus
USB	Upper sideband
UUID	Universally unique identified
VHF	Very high frequency
VNA	Vector network analyzer
VNC	Virtual network computing
WISP	Wireless identification sensing platform
WLAN	Wireless local area network
WPT	Wireless power transfer

Acknowledgements

I want to start off by thanking my advisor Matt Reynolds. I will always be grateful to have worked for and learned so much from you. When I started I didn't know what qualities made for a good advisor but I've been lucky enough to have landed in a great situation. I appreciate everything you've done for me from late night edits, to help with framing research goals, to your endless patience and understanding, and general guidance over the last 5 years.

Thank you to everyone I've worked with in lab at both Duke University and the University of Washington - Jordan Besnoff, Stewart Thomas, Daniel Arnitz, Chris Tralie, Kris Spaeth, Travis Deyle, Seung Yul Shin, Alex Hoang, Eleftherios Kampianakis, Apoorva Sharma, Andrea Pedross-Engel, Xiaojie Fu, Claire Watts, Thang Phu, Vandana Dhawan, Wen-Yung Liao, Sandamali Devadithya, and James Rosenthal. I've enjoyed hearing about all of your research and it's been so helpful to have all of you around to discuss new ideas. I hope I'll always be fortunate enough to work alongside such wonderful and talented people.

I want to say a special thanks to Stewart and Daniel for letting me ask you countless questions. Thank you to my most recent collaborators at UW - Alex Hoang and Thang Phu, my collaborators at Duke - Guy Lipworth, Kushal Seetharam, Da, Huang, David Smith, and Yarolav Urzhumov, and my collaborators at Ricoh Innovations - Ken Gudan, Sergey Chemishkian, Shuai Shao, and John Hull.

Thank you to all of the funding source that have supported my work - National

Science Foundation, Ricoh Innovation, and Lawrence Livermore National Lab.

Thank you to the members of my dissertation committee - John Sahr, Shyam Gollakota, Josh Smith, and Sawyer Fuller. This work is better because of the insightful and helpful questions and comments from all of you.

Finally, I want to thank my mom and dad, my sister Ashley, and brother in law Rico who have all been so supportive during the last 5 years. I'm thankful for all of the time your spent listening to me talking about work, for helping me edit this document, and for being a wonderful escape during countless phone calls. I never would have been able to make it to this point without all of you.

Chapter 1

Introduction

This thesis explores new wireless power and backscatter communication architectures for ultra-low-power wireless sensors and other devices such as wearables. We first present measurement, analysis and harvesting approaches for extracting energy from 2.4 GHz wireless communication signals, including an approach for powering a relatively high power sensor in burst mode at an input power level of -15 dBm. We present the first backscatter-based data uplink approach that achieves compatibility between backscatter devices and billions of completely unmodified standard wireless devices using the Bluetooth Low Energy standard. We show that this data uplink approach can communicate with BLE receivers with a radio communication efficiency of 28.4 pJ/bit. This is over 100x lower energy per bit than conventional BLE transmitters. One microcontroller based implementation consumes over 6x less power than the best commercially-available Bluetooth transmitters, and can leverage both modulated and unmodulated carriers to provide the backscatter uplink. This allows us to transform one BLE signal as a carrier source for another BLE-Backscatter signal.

We investigate the range of the BLE-Backscatter system in both bistatic and monostatic, full-duplex application scenarios. The range analysis considers the BLE receiver sensitivity and performance in the presence of self-jamming interference from the external carrier source in the bistatic case. We also present a carrier cancellation architecture that reduces self-jamming in the monostatic case. We characterize the packet error rate and received signal strength in both cabled and over-the-air scenarios. Finally we present an ultra-low power superheterodyne receiver architecture that leverages an external carrier as the local oscillator, removing the need for on board (or on chip) generation of the local oscillator signal. The receiver uses a two-port mixer for simultaneous mixing and power harvesting of the external carrier and desired BLE signal.

This thesis shows a path toward the widespread adoption of backscatter communication in low-power wireless devices such as smart watches, fitness bands, biomedical sensors, etc. Other wireless devices, such as sensors for the Internet of Things (IoT) where power consumption is a crucial consideration could also benefit from the approaches presented.

1.1 Motivation

With the continued growth of Internet of Things (IoT) devices and wearable technology, reducing the device energy consumption has become a pressing problem. The small form factor that many of these devices require impose restrictions on battery volume, forcing designs to adhere to a small power budget. At the same time, wireless connectivity is an essential function for IoT and wearable devices and one that consumers have come to expect. Recognizing the need for communications with more energy constrained devices, the Bluetooth special interest group (SIG) developed a low power Bluetooth protocol called Bluetooth Low Energy (BLE) or Bluetooth Smart. BLE has been integrated in a variety of wearable products including iBea-

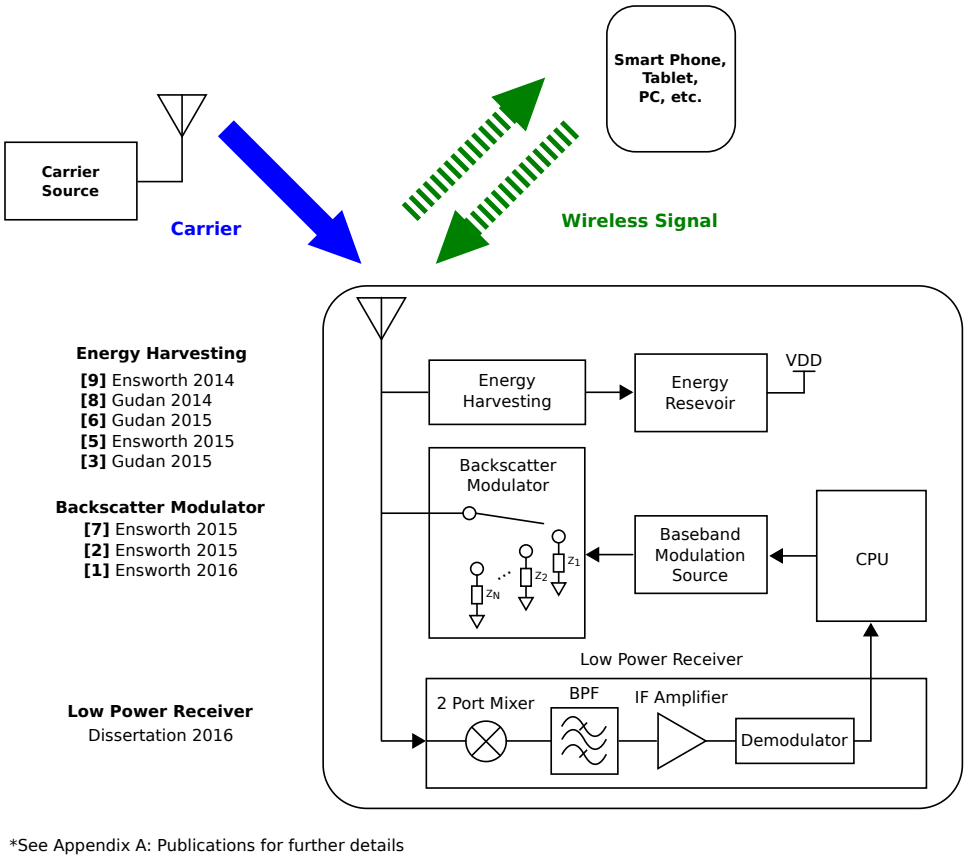


FIGURE 1.1: Battery free wireless device incorporating energy harvesting, low power backscatter data uplink, and a low power receiver architecture for a low power downlink

cons, Apple watch, Nike Fuelband, Microsoft Band, Fitbit Surge, and Pebble Time. Using BLE, these devices are able to pair with smart phones, tablets, or any other nearby BLE compatible devices. This technology is an improvement on the more energy intensive classic Bluetooth but it still requires conventional active radios in both the central and peripheral devices.

An alternative communication technique, far-field modulated backscatter (MBS), can move the power and complexity burden onto a more energy-rich device, such as a smart phone or wireless access point, providing orders of magnitude energy savings during data transmission for small energy-constrained devices. The large

gap in energy requirements per bit of transmitted data between conventional radios and backscatter radios is illustrated in Fig. 1.2. Information about a variety of radios are plotted according to power consumption and data rate. The dotted lines represent lines of constant energy per transmitted bit of data. For the same data rate, backscatter radios are between one and three orders of magnitude more energy efficient than conventional radios.

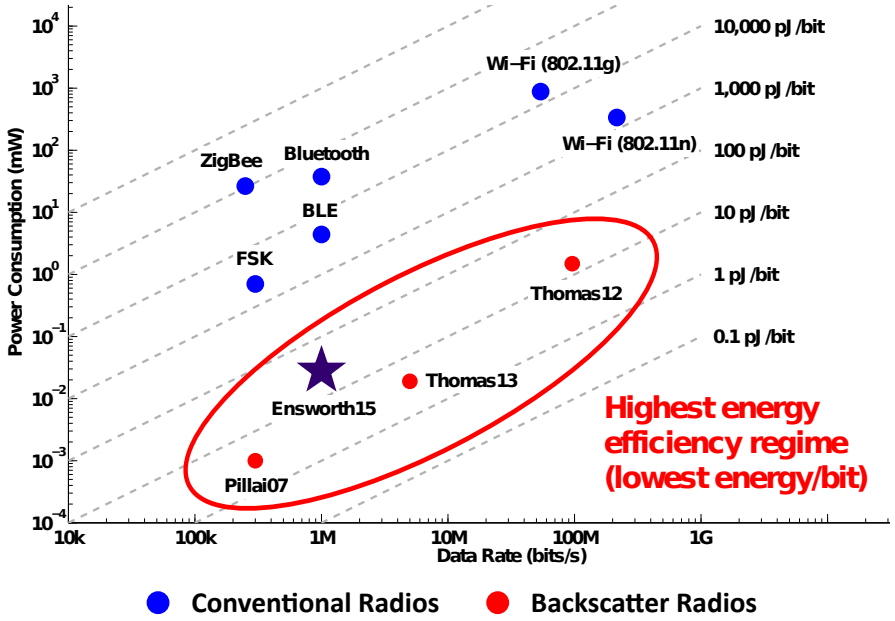


FIGURE 1.2: Comparison of wireless technologies, references in Table 1.1

With the potential energy savings offered by backscatter communication, why isn't long range backscatter incorporated into smart phones? The reason is a combination of size constraints, device complexity, and economic incentives for smart phone manufacturers. Take for example the iPhone 6S. This smart phone already supports wireless communication for Wi-Fi, Bluetooth 4.2, NFC, GPS, GSM, CDMA, and LTE [13]. Adding an additional radio further complicates the design and takes up

Table 1.1: References used for Fig. 1.2

Figure Key	**Radio Type**	**Year**
Ensworth15 [2, 3]	Backscatter	2016, 2015
Thomas12 [4]	Backscatter	2012
Thomas13 [5]	Backscatter	2013
Pillai07 [6]	Backscatter	2007
Wi-Fi (802.11g) [7]	Conventional	2010
WiFi (802.11n) [8]	Conventional	2008
BLE [9]	Conventional	2015
ZigBee [10]	Conventional	2006
Bluetooth [11]	Conventional	2004
FSK [12]	Conventional	2006

valuable board area in the phone. If there isn't a clear economic advantage to introducing a new radio, smart phones will continue to use the set of radios they've already incorporated and monetized. A relatively recent hardware addition to iPhones that meets this criteria is near-field communication (NFC). The inclusion of NFC was driven primarily by a perceived market for mobile payments. Currently, NFC is used by Samsung, Android, and Apple smart phones for their mobile payment solutions.

The influence of the smart phone and tablet market on technology adoption and awareness can be seen in Fig. 1.3, which shows the normalized Google search volume for NFC. Two significant spikes occur in September 2012 and September 2014 that coincide with the announcements of Microsoft mobile wallet and Apple Pay. A small number of hardware manufacturers set the expectations for which communication protocols will become standards. Securing buy-in for a hardware change from the decision makers at these major electronics manufacturers requires a significant market opportunity and is a challenging route for new technology adoption.

Being excluded from smart phones and tablets meant that a special purpose reader infrastructure needed to be developed for the deployment of backscatter devices. Commercial RFID is built around a relatively sparse, expensive custom RFID reader infrastructure with relatively plentiful, inexpensive RFID tags. A concep-

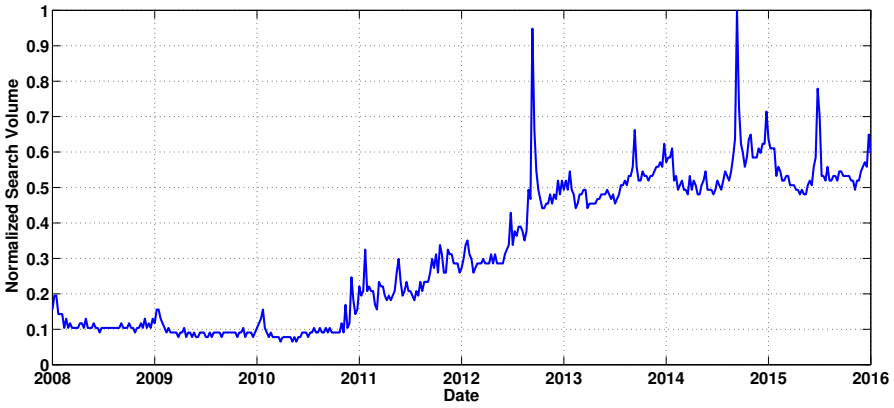


FIGURE 1.3: Normalized Google search volume for the term "NFC"

tual drawing of a traditional backscatter system is shown in Fig. 1.4(a). A dedicated MBS reader transmits a high power continuous wave (CW) carrier signal and a modulated backscatter device selectively reflects the incident carrier by modulating the load presented to its antenna. By switching between two states, binary data can be communicated to the MBS reader with a mutually agreed upon communication protocol.

Recognizing the impediment of sparse MBS infrastructure to MBS adoption, some researchers have worked to reduce the dependency on expensive dedicated RFID readers. One effort was to modify existing wireless communication devices to act like MBS readers. A group in [14] modified a Wi-Fi router to function as an MBS reader but the authors dismissed the idea of directly communicating with conventional wireless devices using backscatter communications, noting that:

> Achieving this capability, however, is challenging since conventional low-power Wi-Fi transceivers require much more power than is available from ambient RF signals. Thus, it is not feasible for RF powered devices to literally speak the Wi-Fi protocol. Conversely, since existing Wi-Fi devices are specifically designed to receive Wi-Fi signals, it is unclear how they would decode other kinds of signals from RF-powered devices.

[14]

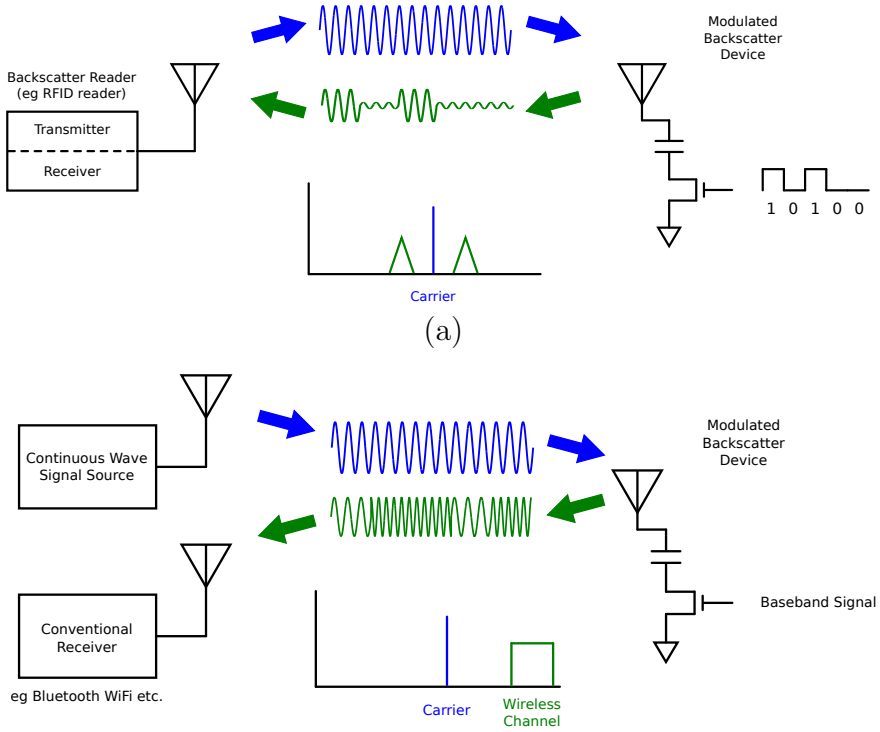


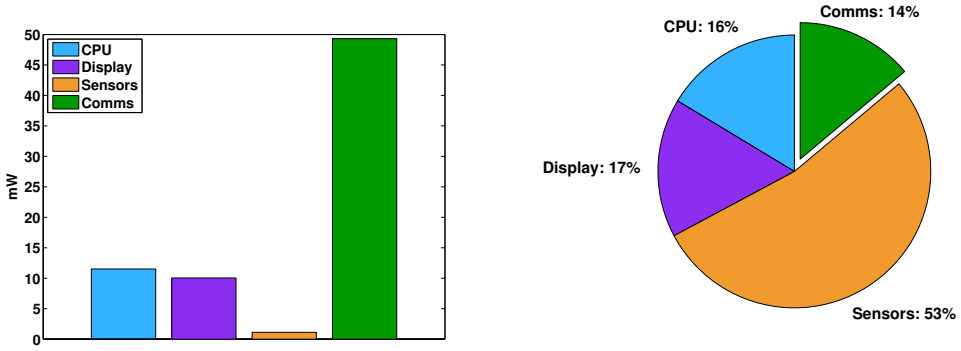
FIGURE 1.4: (a) Traditional view of a backscatter communication system (b) Interoperable view of a backscatter communication system

Our observation was that a backscatter device needs to know what a receiver expects in order to convey information, but it isn't necessary for the receiver to have been designed specifically for modulated backscatter. If the backscatter device can create a signal that is indistinguishable from a conventional transmission, it makes no difference to the receiver how it was generated. This view of interoperable backscatter devices is described in Fig. 1.4(b). A continuous wave signal source can be modulated with a backscatter device to generate a signal that is indistinguishable from the point of view of a conventional wireless receiver. With this scheme, no

hardware, firmware, or software changes are needed for the conventional receiver allowing for low power wireless communication that leverages the existing wireless infrastructure.

Although we believe interoperable communication with conventional wireless communication devices can be useful for a variety of applications such as wireless sensing, inventory tracking, and indoor localization (similar to the Apple iBeacon [15]), the application we will focus on in this document is wearable electronics. These devices have greatly increased in popularity in recent years particularly in the area of health monitoring and smart watches. These connected wearable devices have been explored for some time but had been difficult to produce with commercially attractive battery life, cost, and features [16, 17]. One of the fundamental problems with wearable devices is the competing desire for a small form factor together with power hungry applications. For wearable electronics to be more than a novelty, they have to provide a value to a consumer that justifies the investment of time and money. Partly due to the mobile phone paradigm users expect their devices to be constantly connected. This is a significant challenge for wearable devices because of the power requirements for both transmitting and receiving wireless signals.

To visualize the power consumption breakdown for wearable devices, we consider four subgroups of the wearable fitness monitor the Fitbit Surge: 1. CPU, 2. Display, 3. Sensors, and 4. Communications [18, 19]. For most wearable devices the total energy consumption of each subgroup will depend on the application. For instance, some applications may not call for the display to be on continuously, or may use a subset of the available sensors. As we can see from Fig. 1.5, the most power hungry subsystem in the Fitbit Surge is the communication link. To achieve a long battery life with active communication devices one of the best ways to save energy is to transmit data as infrequently as possible. However, this restricts the functionality of the device.



(a) (b)

FIGURE 1.5: (a) Fitbit Surge power breakdown by subsystem (b) Energy breakdown over a one week period

The Fitbit surge claims a 7 day device lifetime between charges. It uses a 100 mAh 3.7 V battery. Based on that information and the specifications of individual components, we have created a hypothetical use case scenario to see which components consume the most energy. With the accelerometer sensor constantly running, the display in a low power state mode, and the CPU in a low frequency energy conservation mode, there is only enough energy for approximately 5 hours of accumulated display manipulation and approximately 1 hour of wireless data communication per week. Fig. 1.5 shows the power budget for this hypothetical application scenario. Even if the communications system is running at the heavily duty cycled rate of 1 hour per week, it still consumes approximately 14 % of the total energy budget. To achieve a constant communication link for the energy-poor FitBit Surge, the power consumption of the communication link has to be reduced by more than two orders of magnitude. The rest of this document will show that backscatter communication is a viable solution to achieve constant communication with wearable devices.

1.2 Original Contributions

The original contributions discussed in this document include:

- Characterization of available ambient energy in the 2.4 GHz band and harvesting approaches. Published in [20, 21, 22, 23].

- An approach for powering a relatively high power sensor in burst mode at an input power level of -15 dBm at 2.4 GHz. Published in [24].

- The first approach shown to create backscatter signals that are compatible with conventional wireless communication receivers using FSK, PSK, ASK, QAM, and OFDM modulation schemes such as Bluetooth, WiFi, etc. Published in [3, 25].

- The first demonstration of backscatter communication with absolutely unmodified conventional Bluetooth Low Energy receivers (neither hardware nor firmware nor software modifications are required). Published in [3].

- A microcontroller based "BLE-Backscatter" tag that produces band-pass frequency shift keying (FSK) modulation at 1 Mbps, enabling compatibility with conventional BLE receivers. To appear in [26] and Submitted [2].

- A low power receiver approach using an external LO and two port mixer has been demonstrated in a bench top, cabled setup. To be submitted and [27].

1.3 Dissertation Organization

The remainder of this document is organized as follows: Chapter 2 begins with background on research and commercial efforts in wearable technology, including problems that have delayed the widespread adoption of such devices. Section 2.2 outlines related work on MBS. Chapters 3, 4, and 5 contain an analysis of harvesting RF energy in the 2.4 GHz ISM band for the purpose of powering wireless sensors

or other low power devices. Chapter 6 describes how a device that uses backscatter communication can be made compatible with the preexisting infrastructure of wireless receivers, specifically Bluetooth 4.0 Low Energy (BLE) receivers. Background on BLE is covered explaining why this protocol is particularly well suited for backscatter interoperability. The remainder of Chapter 6 discusses the progress to date of our BLE-Backscatter tags including the prototype design choices along with range and energy consumption theory and measurements. Chapter 7 explores the requirements of the carrier signal used for BLE-Backscatter communication. Both unmodulated and modulated carrier signals are used including conventional BLE transmissions as a carrier source for BLE-Backscatter. Chapter 8 characterizes the communication distance achievable for BLE backscatter with a focus on the effects of the carrier signal as a source of interference. A commercial BLE receiver is used to provide measurement data for both the receiver sensitivity and receiver performance with an out of band carrier source acting as a self-jammer. Finally, Chapter 9 describes a low power receiver architecture that takes advantage of the backscatter system's carrier source in place of an on board local oscillator. The two-port mixer used in the receiver is shown to work simultaneously to produce an IF output and a harvested DC output. Combining the backscatter transmitter and low power receiver will allow for a low power bidirectional data link that is important for providing connectivity to wearable devices without imposing a prohibitively expensive power burden.

1.4 Publications

All publications to date are included below.

[1] J. F. Ensworth, A. T. Hoang, T. Q. Phu, and M. S. Reynolds, "Full-Duplex Backscatter System Using a Bluetooth Low Energy (BLE) Receiver", *IEEE Radio Wireless Week* **(To appear)**

[**2**] **J. F. Ensworth** and M. S. Reynolds, "BLE-Backscatter: Ultra-low-power IoT nodes compatible with Bluetooth 4.0 Low Energy (BLE)", *IEEE Transactions on Microwave Theory and Techniques* **(Submitted December 2015, revised August 2016)**

[**3**] K. Gudan, S. Shao, J. J. Hall, A. Hoang, **J. Ensworth**, and M. S. Reynolds, "Ultra-low Power Autonomous 2.4 GHz RF Energy Harvesting and Storage System ", in *2015 IEEE RFID Technology and Applications Conference*, pp. 176-181, September 2015.

[**4**] G. Lipworth, **J. Ensworth**, K. Seetharam, J.S. Lee, P. Schmalenberg, T. Nomura, M. S. Reynolds, D. R. Smith, Y. Urzhumov, "Quasi-Static Magnetic Field Shielding Using Longitudinal Mu-Near-Zero Metamaterials," *Scientific Reports*, vol. 5, August 2015.

[**5**] **J. F. Ensworth** , A T. Hoang, and M. S. Reynolds, "A timer based boost converter for RF energy harvesting", in *2015 IEEE Wireless Power Transfer Conference*, May 2015.

[**6**] K. Gudan, S. Shao, J. J. Hall, **J. Ensworth**, and M. S. Reynolds, "Ultra-low power 2.4 GHz RF energy harvesting and storage system with -25 dBm sensitivity", in *2015 IEEE International Conference on RFID*, pp. 40–46, April 2015.

[**7**] **J. F. Ensworth** and M. S. Reynolds, "Every smart phone is a backscatter reader: Modulated backscatter compatibility with Bluetooth 4.0 Low Energy (BLE) devices," in *2015 IEEE International Conference on RFID*, pp. 78–85, April 2015.

[**8**] K. Gudan, S. Chemishkian, J. J. Hull, S. J. Thomas, **J. Ensworth**, M. S. Reynolds, "A 2.4 GHz ambient RF energy harvesting system with -20 dBm minimum input power and NiMH battery storage," in *2014 IEEE RFID Technology and Applications Conference*, pp. 7–12, September 2014.

[**9**] **J. F. Ensworth**, S. J. Thomas, S. Y. Shin, and M. S. Reynolds, "Waveform-aware ambient RF energy harvesting," in *2014 IEEE International Conference on RFID*, pp. 67–73, April 2014.

[**10**] G. Lipworth, **J. Ensworth**, K. Seetharam, D. Huang, J.S. Lee, P. Schmalenberg, T. Nomura, M. S. Reynolds, D. R. Smith, Y. Urzhumov, "Magnetic metamaterial super lens for increased range wireless power transfer," *Scientific Reports*, vol. 4, January 2014.

Chapter 2

Wearable Technology and Backscatter Communication

2.1 Wearable Technology

Wearable technology is currently in an exciting phase with the recent commercial success of heads up displays (HUDs), fitness trackers, and smart watches. The history of wearable technology, however, predates electronic devices. Eyeglasses, one of the most widespread pieces of wearable technology, were invented in the 13th century. The technology of lenses was used to help people correct their vision. Similarly for people with hearing problems, the ear trumpet was created prior to the use of electronics. These devices may no longer seem as exciting as the modern view of wearable technology, but they had a profound impact for the user and required minimal upkeep.

With the invention of electronics, inventors had new tools at their disposal, and they continued to explore interesting work in the area of human sensory inputs. By utilizing electronic amplification hearing aids became more than just physically large horns designed to collect and funnel sounds waves [28]. Prior to the invention

of the transistor, hearing aids were large, power hungry devices that looked more like old fashioned telephones than the sleek designs now seen worn on or implanted in the ear. For visual sensory input one exciting development owes its start to WWII when pilots needed to simultaneously see what was happening in front of them and acquire electronic data. The solution was the HUD, which projected the data on a see-through display allowing pilots to maintain their field of view and see displayed data. HUDs are currently used in modern military aircraft, some commercial aircraft, and some commercially available cars [29]. One benefit of special purpose HUDs over a wearable device is a less constrained energy source and a specific use case.

While some companies and researchers are focused on creating wearable device platforms, others have approached the problem from the point of view of solving a specific problem. One interesting example is the Smart Hat [30]. This device is designed to alert the wearer that they have entered a hazardous work zone. The hat will beep when it receives a high power RF transmission at the appropriate frequency. If a work zone is illuminated by a highly directive antenna, the beeping will only occur when someone has entered the predefined hazardous zone. Another focused effort with a specific target audience is the Google smart contact lens [31]. The smart contact is designed to aid diabetic users with monitoring their glucose levels by imbedding an energy harvesting unit, glucose sensor, and communication system into a contact lens.

Focusing on a specific target audience for a new technology may help with early adoption issues because the solution can be tailored to a specific problem; the drawback, however, is a limited user population. For general purpose wearable devices such as smart watches there is a larger potential audience but meeting the diverse application requirements for that user base can be challenging while maintaining a useful battery life and aesthetically appealing designs. Applications vary in their requirements for sensors, displays, processing capabilities, communications, and bat-

tery life, but a general purpose device like a smart watch is required to support the extreme use cases for each of these subsystems in a compact design. Adding flexibility for specially built applications gives designers leeway to provide functionality without wasting resources. An example is the display with its colorful touch screen. Some applications used the display in its high power mode but often the display is off or in a low-power static mode. Currently for communications with smart watches the options are a power hungry communication link or no communication. BLE-Backscatter offers another option: dramatically reduced power requirement with a shorter range and the requirement for an external carrier source. This additional communication mode could be a valuable option given its interoperability with currently used conventional communication standards.

2.2 Backscatter Communication

Backscatter communication dates back to 1948 when it was first reported by Harry Stockman as a way of communicating using modulated reflections generated by mechanical devices [32]. Commercial applications of backscatter communication modify reflected signals by implementing load modulation with electronic components. One early commercial application for backscatter communication was automated tolling systems where cars are assigned RFID tags that can be interrogated and read by a reader infrastructure implemented in toll booths. Other commercial endeavors using UHF RFID have largely focused on inventory management. RFID readers are used to query tags and learn the identification information stored on nearby RFID tags.

Recent research in MBS can be thought of as belonging to one of two broad approaches. One approach is to leverage RFID readers and build applications and capabilities around the current EPC Class 1 Generation 2 UHF RFID standard. A second approach is to demonstrate the capabilities of MBS without adhering to any preexisting wireless standards. One of the most widely used research platforms for

working with the current RFID standard is the Wireless Identification and Sensing Platform (WISP) [33]. The WISP is a programmable, microcontroller-based sensor tag that has been used to demonstrate battery free cameras, temperature sensors, capacitive touch sensors, and acoustic sensors [34, 35].

Researchers focused more on demonstrating some of the possibilities of MBS haven't designed around the current RFID standard and have largely used custom MBS reader implementations. A variety of carrier frequencies have been explored for MBS including 2.4 GHz [14, 36], 5.8 GHz [37], 10 GHz [38] and 34 GHz [39] where the physical size of antennas, operating bandwidths, and differing path loss lead to interesting design trade offs and performance for data transfer and localization. Different modulation schemes have also been researched. While the traditional view of MBS has focused on amplitude modulation, 16 QAM MBS at a rate of 96 Mbps has been demonstrated. Backscatter with an FSK modulation scheme have been shown in [40, 41, 42]. Additionally, work has been done with MBS systems that do not rely on a single carrier frequency. TV signals have been used as carriers for backscatter communication by [43, 44] in a concept they call ambient backscatter. The communication signals are selectively reflected by the ambient backscatter tags and those reflections convey information to other nearby backscatter devices.

A similar approach that uses communication signals as the energy source to be reflected has been shown with Wi-Fi. Both [14, 36] produced systems that backscatter data on Wi-Fi transmissions. Instead of having both backscatter transmission and reception performed by backscatter devices, as was the case in ambient backscatter [43, 44], Kellogg et al. [14] used a Wi-Fi access point's channel state information (CSI), and received signal strength indicator (RSSI) to decode backscattered messages. While Kellogg's approach showed that it's possible to decode backscatter messages with Wi-Fi access points, they required MBS devices with relatively large differential radar cross sections and a custom protocol stack running on off-the-shelf

Wi-Fi access points. The Wi-Fi Backscatter device transmits data to a custom protocol stack running on off-the-shelf Wi-Fi hardware by causing a time varying change in the multipath environment surrounding the Wi-Fi device. Because Wi-Fi devices operating according to the IEEE 802.11n specification use a multi-carrier OFDM communication scheme that requires frequent channel estimation to equalize the channel, the time varying multipath caused by the Wi-Fi Backscatter tag is perceived as a time variation in the CSI and RSSI at the Wi-Fi device. A custom protocol stack that interacts with the Wi-Fi chipset uses a statistical signal processing approach to process the CSI and RSSI data and extract the Wi-Fi Backscatter data. A data rate of 1 kbps is reported with a range of 2.1 meters.

We consider the Wi-Fi Backscatter work to be an example of an **"out-of-band"** approach, where the MBS signal is piggy-backed on existing Wi-Fi transmissions using a non-standard protocol stack, requiring access to vendor-specific CSI and RSSI information from the Wi-Fi chipset. A high rate of Wi-Fi transmissions are necessary to serve as a "carrier" for the backscatter signals; in the initial implementation, 30 Wi-Fi packets are needed to transfer a single bit of MBS data [14]. The effect of time-varying multipath due to physical motion of Wi-Fi devices or moving objects such as people is not reported by the authors but seems likely to have an adverse effect on the CSI and RSSI modulation used in that work. The Wi-Fi Backscatter link is bidirectional; data is signaled from the Wi-Fi chipset to the transponder by varying the time interval between Wi-Fi packets being sent. An envelope detector on the transponder uses the presence or absence of a Wi-Fi packet in a given time interval to detect whether a one or a zero is being sent.

In contrast, the work in this document and in [3] presents an **"in-band"** approach to interoperability between a MBS transponder and an unmodified BLE device running an unmodified BLE stack [45]. From the perspective of the BLE device, the BLE advertising packets created by MBS are indistinguishable from a BLE adver-

tising packet sent by a conventional BLE device. They appear in the same channels, with the same modulation scheme, and the same packet formatting. BLE advertising packets (e.g. Apple iBeacons) are designed for unidirectional communication, and [3] accordingly presents a unidirectional uplink. One potential disadvantage of this work is the need for a carrier in the environment at a carefully chosen frequency. This carrier could be supplied by a purposefully deployed transmitter, for example, if the MBS devices were wirelessly powered by that carrier. The carrier is not coordinated in any way with the BLE device or the MBS device, so it can be considered to be an exciter or illumination source for wirelessly powered MBS transponders. We have demonstrated operation at 1 Mbps at a range of 9.4 m using a +15 dBm CW source with an unmodified Apple iPad as the BLE receiving device [3]. With a later microcontroller based implementation described in this document we have demonstrated operation at 1 Mbps at a range of 30 m using a +16 dBm carrier source with an unmodified Apple iPad as the BLE receiving device. A following **"in-band"** approach to interoperability between a MBS transponder and an unmodified Wi-Fi device has been demonstrated in [46]. In experiments with an FPGA-based MBS device backscatter is implemented at all four 802.11b bit rates of 1, 2, 5.5 and 11 Mbps. A simulated IC predicts operating power consumptions of 14.5 and 59.2 μW with data rates of 1 and 11 Mbps respectively.

Chapter 3

Characterizing Ambient RF for Energy Harvesting

This chapter presents a measurement system for characterizing wideband ambient RF energy. The feasibility of using ambient RF energy to power wireless sensors depends on the availability of harvestable energy in the environment. A comprehensive characterization of the available RF energy will inform the design of the harvester and set power limits on any potential networked sensors. By using wideband antennas, logarithmic amplifiers, and a variety of filters on a mobile testing station, we have captured data describing the amount of available energy around a laboratory building on a university campus. We improve on prior work by sampling the output of a log amp with input filters to better approximate the behavior of wide-band diode-based harvesters. We present statistics for available energy in our test location, at frequencies between 700 MHz and 2.6 GHz. We use histograms to understand the distribution of time varying power levels across different frequency bands.

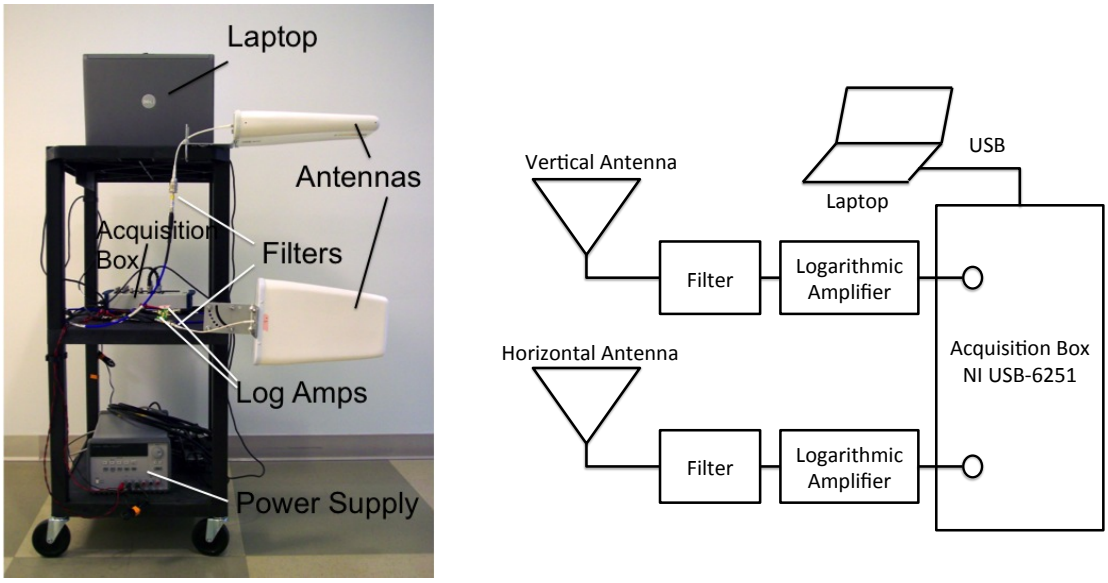
3.1 Introduction

Many efforts in RF energy harvesting begin with selecting potentially interesting signals and designing harvester systems based on sources that are known to have high transmit powers or widespread transmitter locations. Some common signals researched include TV broadcast stations [47, 48, 49], mobile phone base stations [50, 51], Wi-Fi [52, 53, 54], or a specially designed transmitter [30]. Television broadcast stations, mobile phone base stations, and Wi-Fi are ubiquitous ambient RF energy sources and appear to be obvious choices from which to base a harvester's design. An alternative approach is to survey an environment, identify the strongest signals, and then design a harvester based on observations of the RF energy statistics in the environment.

Information regarding the statistics of ambient RF energy would better inform the design of a harvester, leading to a more efficient overall design. We observe that many sources do not have a constant envelope. Many types of digitally modulated RF sources have a strongly bursty character. Wi-Fi signals are a common example of bursty signals with a significant peak-to-average ratio. This chapter offers a method for measuring the statistics of observed ambient RF power levels by utilizing two differently polarized antennas, and a logarithmic amplifier with various input filters to isolate specific communication bands.

3.2 Related Work

Harvesting energy from ambient RF sources has generally focused on three ubiquitous modes of communication: TV broadcast stations, mobile phone base stations, and Wi-Fi. Prototype power harvesters focusing on extracting power from TV signals often require close proximity to specialized RF transmitters, or line-of-sight to high power broadcast stations. One such RF energy harvesting prototype for powering



(a) (b)

FIGURE 3.1: (a) Measurement Cart (b) Block Diagram

ultra low-powered sensors has demonstrated harvesting energy up to 2.55 km from a TV broadcast tower while maintaining line-of-sight [47]. Characterization of DTV signals has also been investigated while maintaining line-of-sight [49]. While useful power can be harvested from TV broadcast stations in line-of-sight, it may not be practical for the deployment of sensor nodes, as each would have to be carefully aligned for proper operation.

Mobile phone base stations are another avenue of ambient RF energy harvesting. In a suburban area, Kitazawa *et al* [50] are able to harvest enough ambient RF energy over periods of 1-3 days to run low-power electronic devices, such as an LCD clock and thermometer, for short amounts of time. These results were obtained in close proximity to a mobile phone base station, within approximately 500 m.

Specialized transmitters offer high energy densities in a small area. High energy densities allow harvesters to operate at high input power levels, but only in a confined operating region. Harvesting ambient energy in a typical office environment, on the other hand, requires a harvester capable of operating at significantly lower input

powers. A harvester operating in the Wi-Fi frequency range would ideally be capable of harvesting voltages even when the incoming RF energy is as low as -45 dBm [52]. In complicated, cluttered, unknown environments where the location and orientation of transmitters are also unknown, the characteristics of ambient RF energy cannot be accurately predicted and must be measured.

Characterization of available ambient RF energy has often been performed with a spectrum analyzer. Baroudi *et al* [55] used a spectrum analyzer to determine if enough ambient RF energy is available to power commercial off-the-shelf (COTS) harvesters and wireless devices. Other methods of characterization have relied on the "max-hold" function on spectrum analyzers [54]. While these measurements reveal the presence of in-band ambient RF energy, information concerning the duty cycle of these signals is lost. The use of a spectrum analyzer in max-hold mode gives a misleading response to bursty, low duty cycle, digital signals. We instead introduce the use of a logarithmic amplifier with input filters to better approximate the behavior of wideband diode-based harvesters.

3.3 Measurement Method

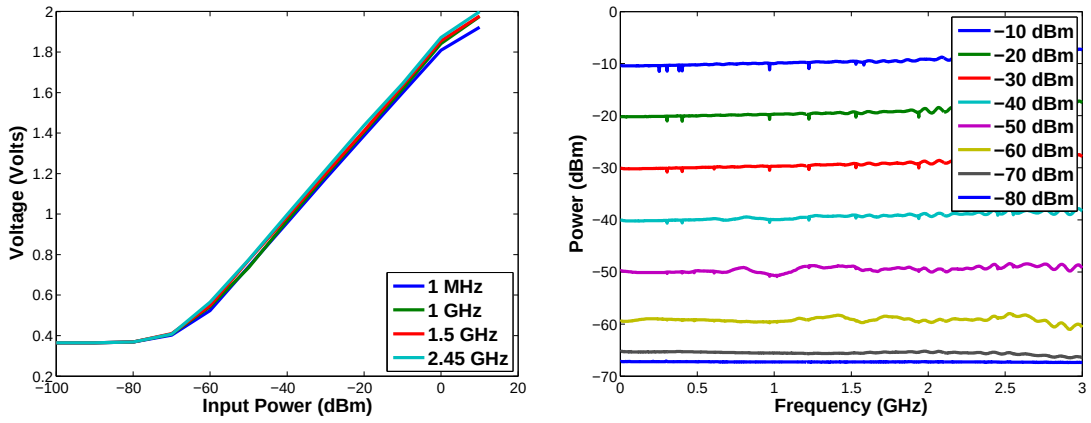
The measurement setup shown in Fig. 3.1(a) is built on a rolling plastic cart so data can be collected anywhere an outlet is accessible. The measurement apparatus features both vertically and horizontally polarized antennas mounted to the cart.

The antennas are connected to filters before delivering RF signals to logarithmic amplifiers, ADL5513 from Analog Devices. The log amps convert the input RF power into a DC output voltage which is then digitized in the NI USB-6251 acquisition box. The acquisition box samples the incoming voltage from the log amp at 8000 samples per second, with 16 bits of resolution. This sampling rate was chosen because we assumed that most practical RF power harvesters would have sufficient bypass capacitance to act as a low-pass filter well below the 4 kHz Nyquist frequency of our

sampler.

Apparatus Components

The logarithmic amplifier is a wide band measurement device and is able to operate from 1 MHz to 3 GHz. Log amps generally exhibit very good amplitude resolution (measured by logarithmic conformance), but they are not frequency selective. By using a log amp, we have approximated the behavior of a wide-band diode based energy harvester which is also not frequency selective within its impedance-matching bandwidth.



(a) (b)

FIGURE 3.2: (a) Log amp Calibration (b) Log amp output power vs. frequency for varying input power levels

The log amp converts RF power to DC voltage, but it needs to be calibrated to determine the correlation between output voltage and input power level. Data for Fig. 3.2(a) was collected by connecting the log amp directly to an Agilent N5181A analog signal generator and recording the log amp's DC output voltage on a multi-meter. Fig. 3.2(a) shows that between -60 and 0 dBm input power, the log amp is operating in its log region. Plotting a line of best fit for the input power and output voltage created a mapping to convert the log amp's output voltage to an input power measurement. The log amp has a very flat response over frequencies from

1 MHz to 3 GHz. The variation in power vs. input frequency seen in Fig. 3.2(b) can be explained by the increased loss at high frequencies in the cables connecting the antennas to the log amp. In both Fig. 3.2(a) and Fig. 3.2(b), the noise floor of our measurement system can be seen to be approximately -67 dBm.

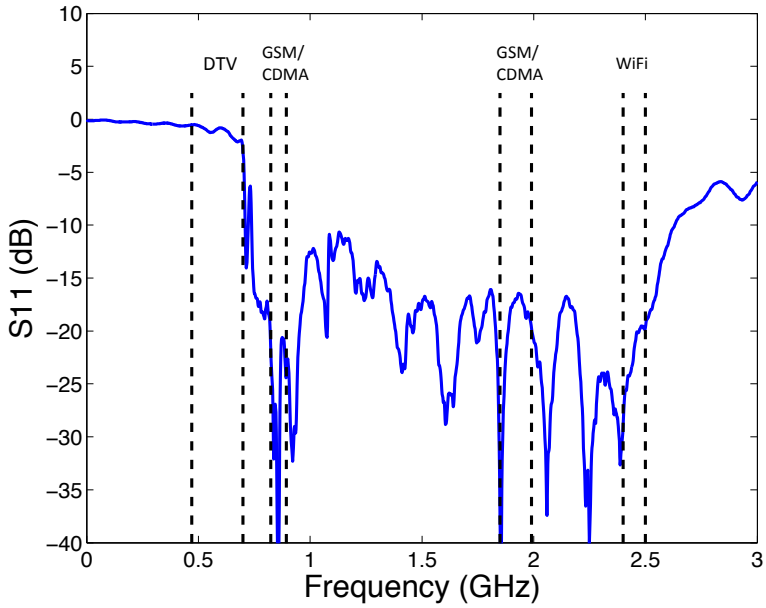


FIGURE 3.3: Return Loss

The antenna selected for the measurement apparatus is an 11 dBi log periodic yagi antenna, L-Com HG824-11LP. As seen in Fig. 3.3, the return loss for this antenna shows an operating range from 700 MHz to 2.6 GHz. This antenna is suitable for measuring signals from the Global System for Mobile Communications (GSM), Wireless Local Area Network (WLAN), and Wi-Fi, all of which are widely used and have been investigated in previous work [56].

Three filters were used separately in the measurement apparatus to isolate the frequency bands measured by the log amp. By using each of the three filters characterized in Fig. 3.4, the RF energy source's frequency information can be observed along with the amount of ambient energy available. The measurement system's antenna and 1 GHz LPF block signals from both DTV and Wi-Fi and pass signals

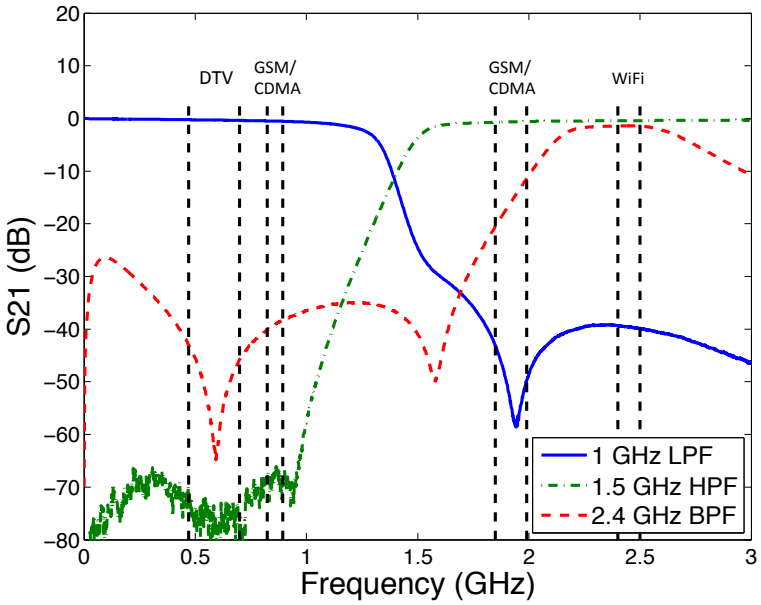


FIGURE 3.4: Filter Frequency Response

between 700 MHz and 1.3 GHz, a frequency range that captures the lower section of the GSM/CDMA band. The measurement apparatus's effective bandwidth with the HPF is from 1.5 - 2.6 GHz. This window encompasses both the higher section of the GSM/CDMA band and Wi-Fi. The 2.4 GHz BPF was chosen to provide information about the available ambient Wi-Fi power while filtering out signals from GSM/CDMA. With the amount of Wi-Fi traffic in a typical university building, this frequency band was expected to yield a large portion of the total available ambient RF energy.

Log amp Advantages

Both a log amp and a spectrum analyzer can be used to observe the energy received from an RF signal. For signals with high duty cycles, there is little difference between the two approaches, but for low-duty-cycle spikes we have found that a sampled log amp is more representative of the behavior of diode based energy harvesters. The following example of measuring the total received energy during a 30-second time

interval illustrates the benefits of the log amp.

Using the horizontally polarized antenna and power splitter, Mini-Circuits ZAPD-4-S+, RF power was received and split evenly between a log amp and a spectrum analyzer, Agilent N9320B. The 2.4 GHz BPF was placed after the antenna to isolate the Wi-Fi band. A "max-hold" and log amp measurement were taken over the same 30-second time interval.

To compute the energy in Joules in a given bandwidth as measured by the spectrum analyzer, equation 3.1 was used:

$$E_{SA} = \left[\int_{f_1}^{f_2} \left(P_{SA} - RBW \right) \, df \right] t \tag{3.1}$$

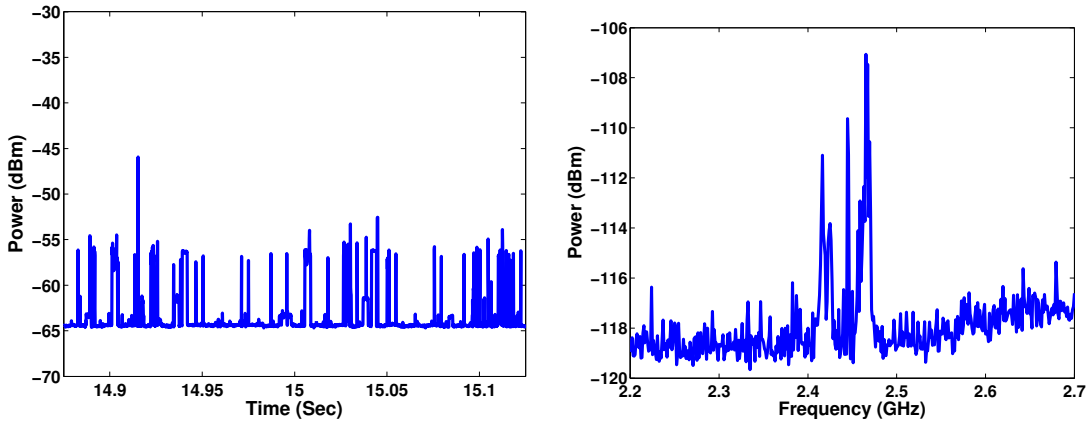
Here, P_{SA} is the power reported by the spectrum analyzer at each frequency, RBW is the resolution bandwidth, f_1 and f_2 are the lower and upper frequency, respectively, and t is the time over which the energy reported by the spectrum analyzer, E_{SA}, is computed. The quantity $P_{SA} - RBW$ must be in linear units to accurately determine E_{SA}.

The energy reported by the log amp is calculated using equation 3.2:

$$E_{LA} = \sum^{N} P_{LA} \frac{1}{F_s} \tag{3.2}$$

E_{LA} is the energy, in Joules, captured by the log amp during a given time interval, N is the total number of samples, P_{LA} is the power level, in Watts, reported by the log amp using the calibration curve in Fig. 3.2(a), and F_s is the sampling frequency of the NI USB-6251 acquisition box.

The total energy reported by the log amp over the 30-second interval is 24.7 nJ compared to 26,800 nJ reported by using the max hold function of the spectrum analyzer. The energy calculation with the max hold drastically overestimates how



(a) (b)

FIGURE 3.5: (a) Closeup view of 30-second log amp data capture (b) Max hold adjusted for 100 kHz RBW, as reported in [1]

often high power signals are present. Fig. 3.5(a) shows a 0.25 second interval of the 30-second measurement from the log amp. A signal with a low duty cycle can be seen on this time scale and since each 125 μs sample interval is taken into account in the log amp's energy calculation, the duty cycle has very little impact on the reported energy. The max hold energy calculation, on the other hand, becomes less accurate as the duty cycle of the measured signal decreases. In a similar manner, max hold calculations over long time intervals heavily skew energy measurements by reporting high power outliers.

3.4 Example Results

Measurements were taken from 6 locations as depicted in Fig. 3.6. All 6 locations are inside the university building on the 3rd floor. Measurements were performed in the hallway near each numbered room, except for the measurement at 3418 which was taken inside a lab. At each location, measurements were taken in 30-second intervals with the antennas facing 4 directions – North, East, South and West – to increase the area covered by the directive antennas. Additionally, data was collected

with each filter described in Fig. 3.4. In total, there are 12 minutes of log amp measurements collected with each of the 3 filters as part of the measurement system. The measurements were collected between 9:00AM and 5:00PM.

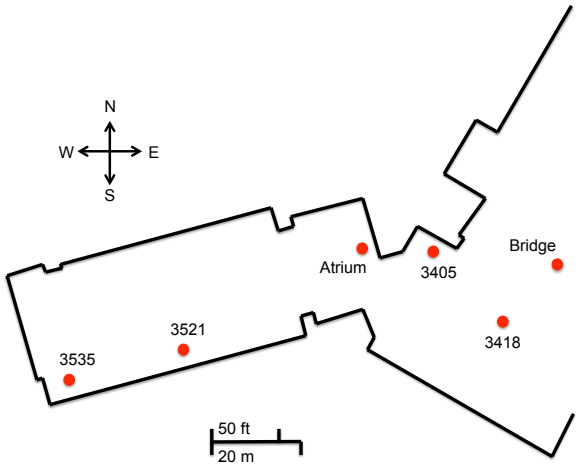


FIGURE 3.6: Measurement Locations

All 12 minutes of data were combined to calculate histograms and cumulative distribution functions (CDFs). As can be seen in Fig. 3.7, much higher power levels were observed in measurements taken with the 1 GHz LPF. While there doesn't appear to be a significant difference between the horizontal and vertical antennas in Fig. 3.7(c) or Fig. 3.7(e), there is a clear vertical polarization preference in Fig. 3.7(a).

The CDF in Fig. 3.7(b) more clearly illustrates the difference in received power based on antenna polarization. The median received power at the vertical antenna is approximately 8 dB higher than the horizontal antenna after passing through the LPF. There is an even larger difference, approximately 15 dB, for the highest 5 % of received signals depending on the antenna's polarization, with a preference for vertical polarization.

The signals within the 2.4 GHz passband have lower total power than signals in the 1.5 GHz - 3 GHz range. Fig. 3.7(d) and Fig. 3.7(f) show similar probabilities of receiving a signal above -45 dBm, but there appears to be a source, out of band for

the 2.4 GHz BPF, that is contributing powers between -60 and -45 dBm when using the HPF. Another observation about Fig. 3.7(f) is that half of the measurements from the 2.4 GHz BPF are at the noise floor of the log amp. Due to the noise floor of the log amp, signals with a power level of -67 dBm or below are reported as -67 dBm.

Figs. 3.8(a)-3.8(e) shows one minute of recorded power with each filter. Figs. 3.8(b)-3.8(f) are closeup views of the same time domain power display, 120 ms in duration. Zooming in on the power time series collected with the 1 GHz LPF doesn't reveal much about the composition of the signal, but Fig. 3.8(d) and Fig. 3.8(f) shows the existence of fine detail in the waveform. This is the same information that is glossed over by the max hold option of spectrum analyzer measurements.

The received power above 1.5 GHz is much more volatile than the received power between 700 MHz - 1.3 GHz. The bursty nature of the higher frequency signals is evidenced by the frequent power spikes. The range of the power fluctuations is much higher in Fig. 3.8(f) than Fig. 3.8(d). These power fluctuations could be due to low duty cycle communication. Even if an energy harvester could operate at these low power levels, they would only be able to produce an output voltage during very brief windows. The harvester's output voltage would fluctuate rapidly with the time varying power source.

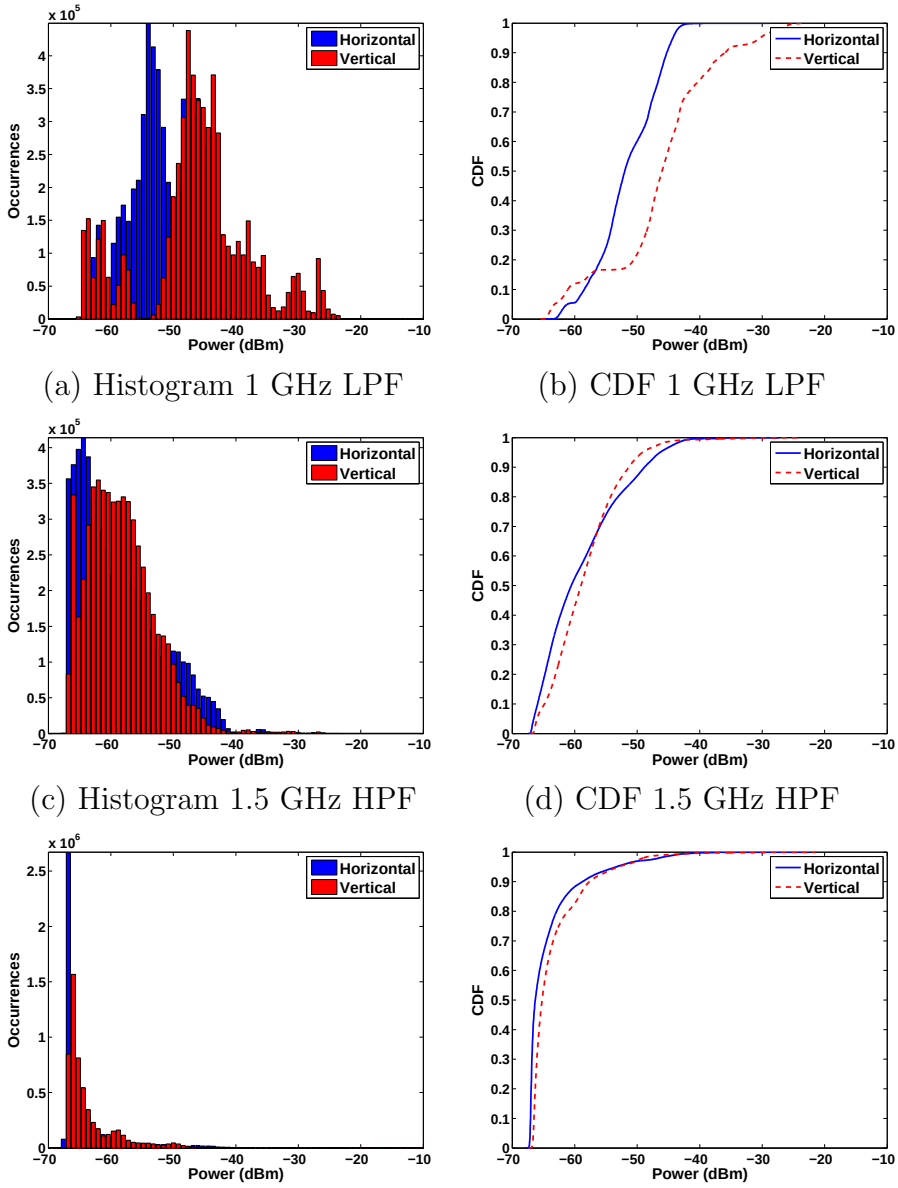
A single short-time high-power spike in Fig. 3.8(c) exists around 40 seconds with a horizontally polarized power of approximately -27 dBm, and a vertically polarized power of approximately -35 dBm. The magnitude of this power spike is significantly greater than the average power in this time series, and it occurs infrequently at these high frequencies, which is also shown in Fig. 3.7(c). The BPF filter attenuates more frequencies than the HPF, but still shows a similar bursty nature in the signals that fall within the 2.2 - 2.6 GHz band. The signals within this band spend the majority of the time at a very low power level, around -63 dBm, and have quick power spikes before returning back to the "base" power level. The duty cycle of the power spikes

captured by the BPF is lower than those captured by the HPF.

3.5 Chapter Conclusion

In this chapter, we have presented a method for measuring the statistics of wide-band ambient RF energy. While this work focused on a laboratory building on a university campus, the measurement method can be applied to various environments. Using both horizontally and vertically polarized antennas, logarithmic amplifiers, and a variety of filters, the characteristics of ambient RF energy in specific bands were captured and analyzed. The fluctuation of RF power over time is shown in different frequency bands. This information can aid in the design of an efficient harvester, and sets power limits on networked sensors. We show improvement over prior measurement methods by utilizing a logarithmic amplifier together with input filters to better approximate the behavior of diode-based harvesters. We've shown that in a laboratory building on a university campus that there is a significant vertical polarization preference from 700 MHz - 1.3 GHz and that power availability is greater here than in the range from 1.5 - 2.6 GHz. The bursty, low duty cycle nature of signals in the 1.5 - 2.6 GHz band, which includes Wi-Fi, was also revealed.

Depending on the achievable bandwidth of a power harvester's matching network, narrower BPFs could be added to the measurement apparatus to calculate the statistics of harvestable signals. Recording measurements in more locations, including outdoor locations, will give a better picture of where ambient harvesters could be successfully deployed. One way to enhance the data collected by the measurement apparatus is to use an analog to digital converter with a higher sampling rate. The 8 kSps sampling rate limited the frequency of power variations that could be observed. Lastly, a power harvester could be added to the measurement cart along with a 10 dB coupler so both the received power levels and harvested voltages could be recorded simultaneously.



(a) Histogram 1 GHz LPF

(b) CDF 1 GHz LPF

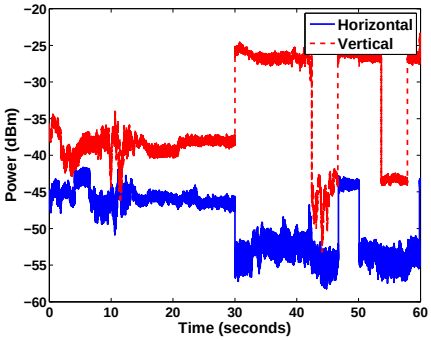
(c) Histogram 1.5 GHz HPF

(d) CDF 1.5 GHz HPF

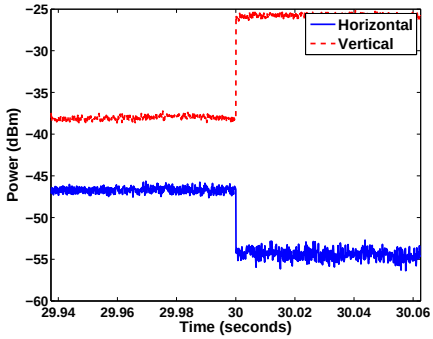
(e) Histogram 2.4 GHz BPF

(f) CDF 2.4 GHz BPF

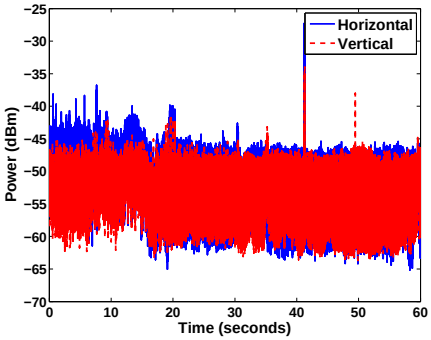
FIGURE 3.7: Power Statistics



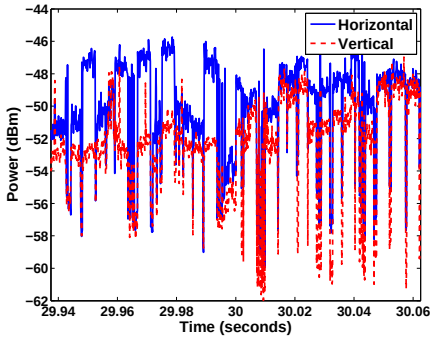
(a) 1 GHz LPF



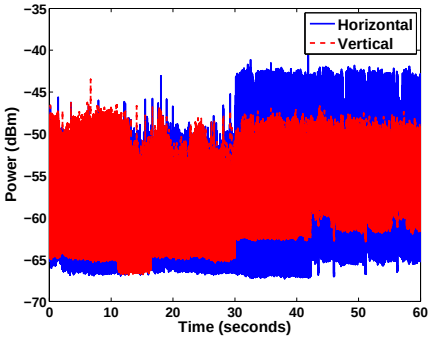
(b) Zoomed view of 1 GHz LPF



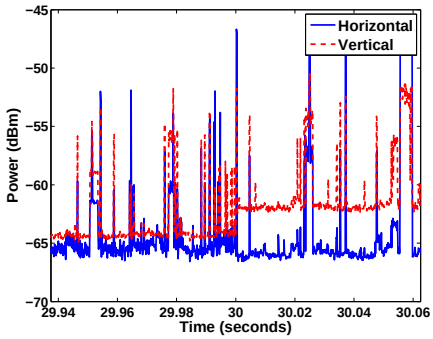
(c) 1.5 GHz HPF



(d) Zoomed view of 1.5 GHz HPF



(e) 2.4 GHz BPF



(f) Zoomed view of 2.4 GHz BPF

FIGURE 3.8: Time Domain Plots

Chapter 4

Waveform-Aware Ambient RF Energy Harvesting

In this chapter we suggest a new class of RF energy harvesters, which we call waveform aware harvesters. In contrast to traditional rectenna designs, which are usually designed for high efficiency with continuous wave (CW) signals, waveform aware harvesters are RF to DC converters which are optimized for their performance with non-CW signals. We suggest that waveform aware harvesters may have significant advantages in ambient energy harvesting, where the available RF energy is in the form of communication waveforms of a variety of types. We present an initial proof-of-concept demonstration of a waveform aware harvester optimized for harvesting energy from 2.4 GHz Wi-Fi (802.11b/g) signals with a realistic traffic model. Under realistic traffic conditions, 802.11b/g client transmissions are bursty, with a high peak-to-average ratio and a low duty cycle. We demonstrate optimized recovery of harvested energy from single 802.11b/g transmission bursts on the order of 1 ms in duration. We present an expression for maximizing usable energy stored in an energy reservoir given a signal model and parameters of the energy-harvester circuit. In contrast to other work where assumptions of CW sources lead to the desirability of

a large storage capacitor, our approach considers the existing communication signal model and optimizes capacitor size to maximize the stored usable energy for a short transmission burst.

4.1 Introduction

A critical aspect of any wireless power transfer (WPT) system is the rectifier, or energy harvester, which converts incoming radio frequency (RF) energy to a usable form, usually a DC voltage. The conversion from RF to DC energy can be performed by circuits of a wide variation in complexity, ranging from single Schottky diodes to complex circuits employing maximum power point tracking (MPPT) or controlled synchronous rectification of the RF signal.

Often, the term energy harvester is used for circuitry which encompasses both the initial RF to DC conversion (e.g. as performed by a diode), some form of power reservoir, such as a capacitor, supercapacitor, or a rechargeable battery, and some form of supervisory circuit, such as a threshold comparator which supplies a wake-up signal when sufficient energy has accumulated in the reservoir to perform a useful task. The critical properties of an energy harvester include its ability to harvest energy efficiently from available RF signals, its ability to store the harvested energy efficiently with minimal storage loss, and its ability to make the stored energy available to meet the voltage, current, and duty cycle requirements of a desired application. In this chapter we are focused on WPT systems operating in the VHF, UHF and microwave regime, but these general harvester properties also apply to WPT systems operating in the LF and HF regimes as well.

WPT systems can be broadly divided into two overall categories or types. The first type is the purpose-built WPT system which includes a custom wireless power transmitter to supply the RF energy being transferred to a harvester, often a rectifier-antenna combination called a rectenna [57]. The second type is the ambient energy

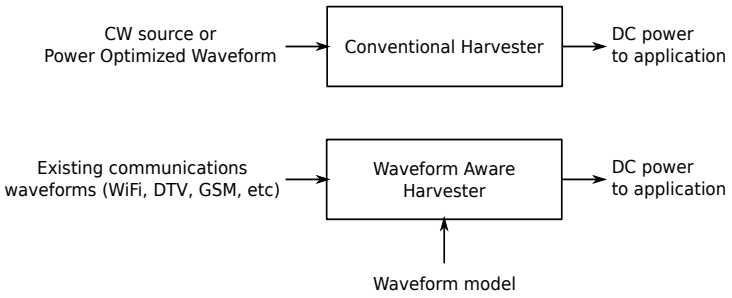


FIGURE 4.1: Harvester Types: (a) Conventional (b) Waveform Aware

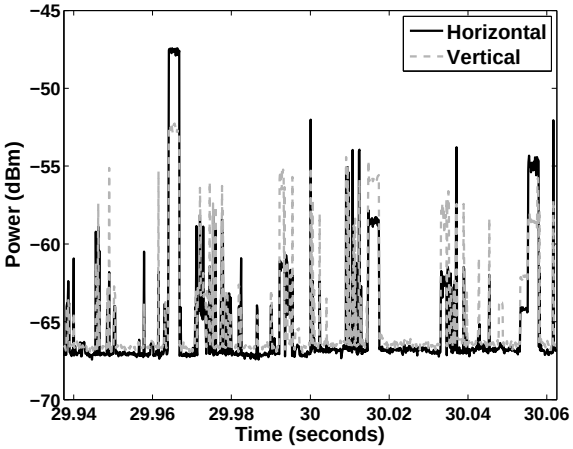


FIGURE 4.2: Time domain plot of indoor 2.4 GHz energy from a Wi-Fi network, measured with vertically and horizontally polarized 6 dBi antennas, showing bursty traffic from multiple sources

harvesting case, e.g. [58, 47, 59], where signals of opportunity that are already present in the environment are harvested.

A key distinction between these two classes of WPT systems is the ability of the WPT system designer to control the waveform being transmitted. In the purpose-built case, the WPT system designer has free choice of the transmitted waveform and power levels, within the limitations of regulatory requirements (e.g. FCC, ETSI, etc) and the limitations imposed by human electromagnetic exposure regulations. In the ambient energy harvesting case, the WPT system designer must work around the waveforms and power levels that are already present in the environment.

In this chapter we introduce the concept of the waveform aware harvester as shown in Fig. 4.1, targeting the ambient energy harvesting case. We present a specific proof-of-concept where an 802.11b/g waveform with actual network traffic as shown in Fig. 4.2 is incorporated into the design of a 2.4 GHz diode-based harvester. The proof-of-concept harvester is shown in Fig. 4.3 and Fig. 4.4. We consider harvester optimizations including maximum power-point tracking (MPPT) as well as reservoir capacitor selection to maximize useful harvested energy given an existing communication waveform having a bursty traffic model with transmissions on the order of 100μs to 1ms. We consider the nonlinear behavior of the diode itself, as well as the requirements of a typical application load requiring one of two power-up threshold voltages: (1) $V_{TH} = 0.8$ V, as is typical for CMOS logic, and (2) $V_{TH} = 50$ mV, as is typical for ultra-low startup voltage boost converters using JFETs [60, 61, 62, 63]. While we have based our original implementation around a voltage-doubling diode configuration, our approach is equally applicable to any number of voltage multiplier stages with suitable adjustment for the maximum power point of each harvester.

As shown in Fig. 4.5 we define *usable energy* as energy stored in a reservoir capacitor with its terminal voltage exceeding V_{TH}. We derive an expression for the useful-energy-maximizing reservoir capacitance C_X as a function of ambient RF signal duty cycle and the load impedance R_L at a diode harvester's maximum power point.

4.2 Related Work

The work presented in this chapter is focused on ambient energy harvesting, where the available RF energy is originally intended for some other purpose, usually for communication. Many examples of ambient RF energy harvesting systems have recently been developed. Examples of commonly-harvested ambient RF energy sources include digital television (DTV) broadcasts [58, 48, 64, 65], cellular base station

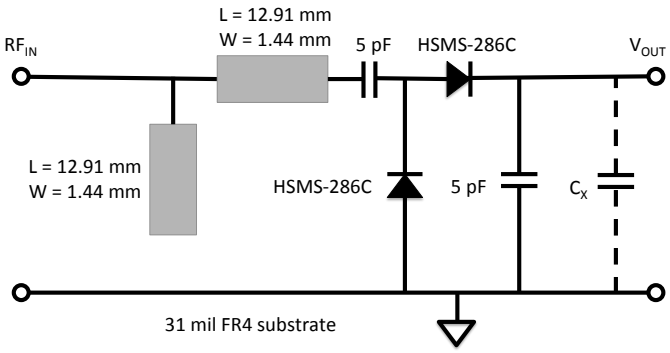


FIGURE 4.3: Diode based harvester schematic

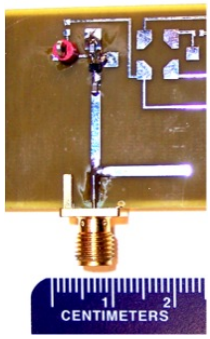


FIGURE 4.4: Photo of diode based harvester

transmissions (GSM / CDMA) [51, 56], Wi-Fi transmissions [54, 53, 1], among others.

While some of these transmissions are generally continuously available (e.g. DTV broadcast, which is usually continuous except during maintenance periods), other transmissions such as GSM and Wi-Fi are bursty and transmission duty cycle (and thus average power) varies with communication traffic [50, 49]. In this work, we consider the bursty traffic case, and show how the harvester can be optimized given a waveform and a particular traffic assumption. We present a first proof of concept based on a static optimization of reservoir capacitor value C_X for a particular operating point, which has the drawback of optimality only in a limited operating

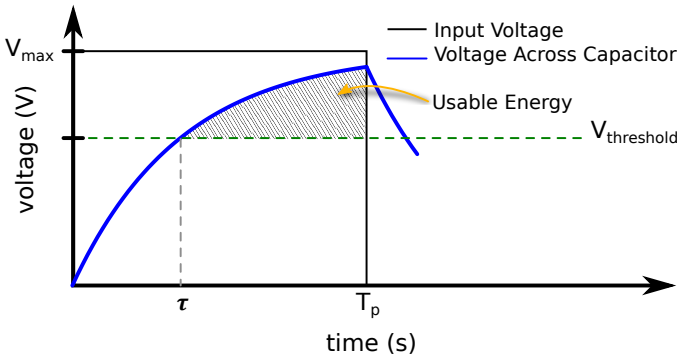


FIGURE 4.5: Cartoon view of the usable energy stored in capacitor C_X during one transmission burst of duration T_p

regime.

Fortunately we observe that this approach yields a fairly stable optimum and thus a wide tolerance in the value of C_X. Alternative implementations based on switched capacitors, with a circuit implementation analogous to the ultracapacitor switching scheme presented in [66], may offer a good compromise between efficiency gains at the optimal point, and the energy consumed by a dynamic optimization algorithm.

4.2.1 Comparison with Power Optimized Waveforms (POWs)

In the purpose-built WPT system case, prior research has shown that there can be significant advantages to co-designing the transmitted waveform given a particular RF energy harvesting circuit. Because diode-based RF energy harvesters have nonlinear I-V curves, they exhibit a threshold effect where RF-DC conversion efficiency is much higher once the incident RF power (and thus the instantaneous RF voltage across the diode) exceeds some threshold that is a function of diode properties. Waveforms including Gaussian-shaped pulses and raised cosines (examples of so-called "Power optimized waveforms" or POWs) [67, 68, 69], multi-sines [70], and chaotic signals [71] have all been designed to exhibit favorable properties such as high peak to average power ratios. For example, it has been shown in simulation [69] that

multicarrier POWs, harvested by realistic diode models, could yield over 20dB improvement in harvestable power over the CW case, albeit with a significant penalty in waveform bandwidth (250 MHz vs. essentially zero for CW). The POW work has shown that designing the transmitted waveform with knowledge of the behavior of the harvester can yield a significant advantage in harvester performance.

The work described in this chapter addresses the dual of the POW design problem- in the POW design problem, the harvester is given and the waveform is optimized to drive it. In the work presented here, the waveform is given and the harvester is optimized to function with that waveform.

4.2.2 Comparison with Maximum Power-Point Tracking (MPPT) approaches

There is a substantial literature in MPPT and application duty-cycle management for harvested-energy systems, including for RF powered systems. MPPT is best known in solar photovoltaic (PV) system applications. In both the PV and RF harvesting applications, the harvesting element is a diode with a nonlinear I-V curve. Because the diode is a nonlinear device, the power delivered to the load varies dramatically with load impedance. The MPPT circuit functions as a load impedance converter to maximize the power delivered to the load, given a particular nonlinear operating point.

The challenge in the RF harvesting case, compared to the PV case, is designing a MPPT circuit that will operate at the much lower incident power densities typical of the RF harvesting case (usually 10^{-5} to 0.1 W/m^2 for ambient RF, compared to 1500 W/m^2 in the PV case. Several examples of low-power MPPT systems are described in [72, 73, 74, 75].

For example, the system described in [72] targets harvesting of ambient RF signals from a cell-phone tower. This system includes a microprocessor-based power management controller employing a dual-mode continuous / discontinuous switch-

mode DC-DC converter at the output of the rectifying diode. This DC-DC converter is used to accomplish MPPT and to deliver a charging current to a lithium battery. One disadvantage of this approach is the relatively high power consumption of the microcontroller and the switch-mode gate drive oscillator. The power management controller is shown to have a net advantage in charging energy delivered to the battery for incident RF powers of 125 μW (-9 dBm) and 250 μW (-6 dBm), and to represent a net loss of efficiency for incident RF power substantially lower than those levels. The work presented here is focused on incident power levels of less than 50μW (-13 dBm), well below the power levels where existing MPPT solutions have shown a net advantage.

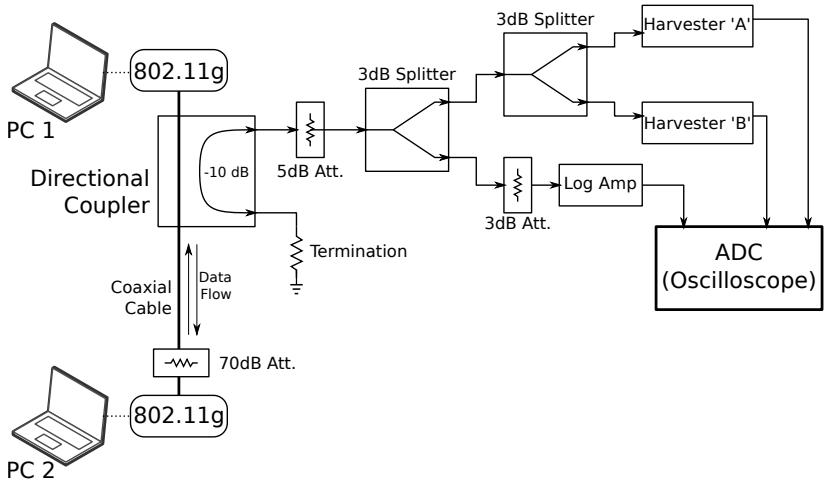


FIGURE 4.6: Benchtop 802.11b/g traffic testbed schematic

4.2.3 Comparison with Duty Cycle Management algorithms

Duty-cycle management refers to harvested-energy systems in which the application duty cycle varies in response to available energy over a period of time, usually seconds to hours. Most harvested-energy systems make use of duty cycling at varying levels of sophistication. The system described in [65] presents an example of two

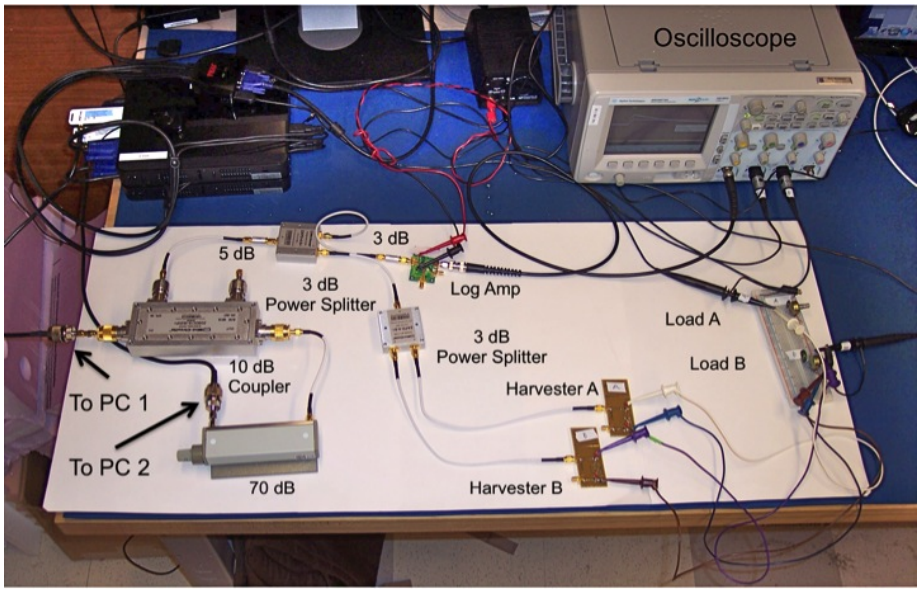


FIGURE 4.7: Photo of the benchtop 802.11b/g traffic testbed

alternative duty-cycle management algorithms in an RF-powered sensor scenario. In this example, energy is harvested from incoming digital television (DTV) signals and dissipated in a combination of capacitor leakage and microprocessor operating current over time periods of seconds to minutes. A dynamic control strategy is proposed which updates the microprocessor run-time every few minutes in response to changing conditions. The authors' data-driven simulations indicate that with a simple linear-quadratic (LQ) strategy, 73.2% of harvested energy can be used for the sensing task, while an improved model incorporating capacitor leakage improves sensor task energy utilization to 74.6% of harvested energy.

The work presented in this chapter is distinct from [65] because storage capacitor selection C_X is optimized on the time scale of network traffic for the signal being harvested, usually on the order of 100 μs to $\approx$ 1 s.

4.3 Wi-Fi Traffic Testbed

In order to perform repeatable experiments when developing harvesters for ambient Wi-Fi signals, we have constructed a benchtop testbed as shown in Fig. 4.6 and 4.7. This testbed is designed to allow experimenting with representative signal levels and traffic in a connectorized environment to ensure repeatability. Two Asus eeePCs running Ubuntu Linux (PC #1 and PC #2) are set up with USB 802.11b/g adapters that have been modified with SMA connectors in place of their internal antennas. The Wi-Fi adapters are both configured to Channel 7 (2.442 GHz center frequency), while the output power of the USB Wi-Fi adapter can be set as high as +15 dBm. Attenuation of 70 dB is employed between the two Wi-Fi adapters. A sample of the transmitted signal from PC #1 is obtained using a 10dB directional coupler, and this sample is then split into two paths. The 5 dB attenuator shown at the output of the directional coupler was varied to permit harvesting measurements at varying incident power levels. In the experiments presented in this chapter, incident RF levels of -8 dBm and -21 dBm at the harvester were used as two standard conditions.

The sampled signal path is further split to two harvesters, **A** and **B**. The second path is fed to an Analog Devices ADL5513 logarithmic amplifier selected because of its excellent log conformance over 80dB of dynamic range, and fast rise/fall time of around 20 ns [1]. An Agilent MSO6014 oscilloscope is used to simultaneously sample the harvester and log amp outputs. The log amp was calibrated over its entire dynamic range by reference to an Agilent N5181 MXG signal generator. Network traffic is generated using VNC, FTP, and open-source tools supplied with WireShark (www.wireshark.org).

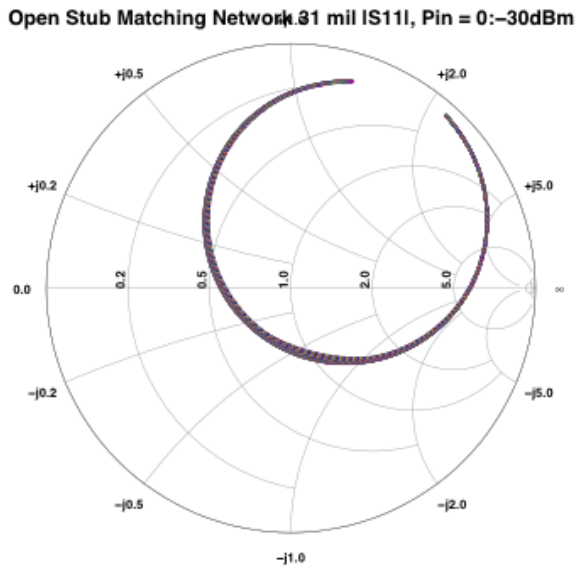


FIGURE 4.8: Measured S11 of the harvester from 2.3 GHz to 2.6 GHz

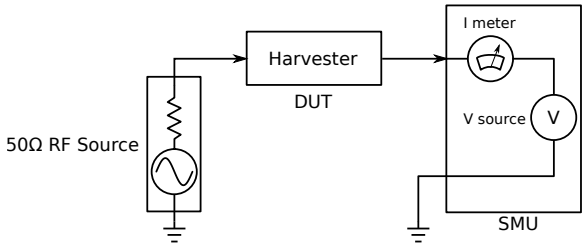


FIGURE 4.9: Maximum power point measurement setup

4.4 Diode-based harvester characterization

The harvester shown in Fig. 4.3 and Fig. 4.4 was designed to be well matched at input power levels below -20 dBm where the majority of ambient Wi-Fi signals are expected to fall. The harvester was characterized both in terms of its input match from 2.3 GHz to 2.6 GHz, as measured with an Agilent E5062A VNA and shown in Fig. 4.8, as well as for harvesting efficiency at its maximum power point (MPP). Harvesting efficiency is defined as the ratio of input RF power at the harvester to harvested DC power at the load ($\eta = P_{DC}/P_{RF}$).

To perform the MPP measurement, a Keithley 2401 source-measure unit (SMU)

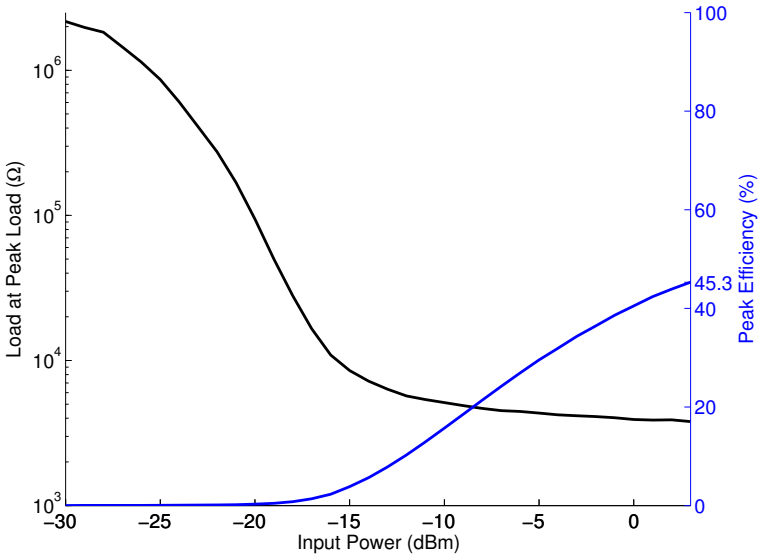


FIGURE 4.10: Measured maximum power point curve for the 2.4 GHz harvester

was connected to the harvester, which was driven from an Agilent N5181A MXG signal generator. A Matlab script controlled both instruments and the I-V curve of the harvester was extracted at each input power level. At each input power level, the optimal load resistance R_L was calculated from the I-V curve and plotted in Fig. 4.10. The peak efficiency of the harvester was measured at around 45.3% with a load resistance of around 5 kΩ at 3 dBm, which is due to the impedance match being optimized for much lower input power levels. A higher peak efficiency could be obtained if the harvester were re-matched for the 3 dBm input level, but this level is much higher than would be expected from the ambient harvesting case given the signal levels shown in Fig. 4.2. In the expected ambient RF signal harvesting regime below -20 dBm, the MPP occurs at load resistances of the order of 100 kΩ. This MPP curve was stored in Matlab and used to create a table-lookup based MPP tracker in the experiments to follow.

4.4.1 Time-domain response of the diode-based harvester

Because of this work's emphasis on harvesting bursty 802.11b/g signals, the time domain response of the harvester was compared with the calibrated ADL5513 log amp. Fig. 4.11 shows the response time of two nearly-identical harvesters **A** and **B** responding to the same 802.11b/g signal. In this figure, the load on each harvester diode consisted of the 5 pF RF bypass capacitor in parallel with a 250 kΩ resistance and a 1 MΩ//10 pF oscilloscope probe. With this high impedance (200 kΩ), low capacitance (15 pF) load, each harvester developed around 80 mV when driven by an 802.11b/g transmission at -21 dBm, and the rise and fall times of the harvester output were negligible compared to the ≈1 ms transmission duration.

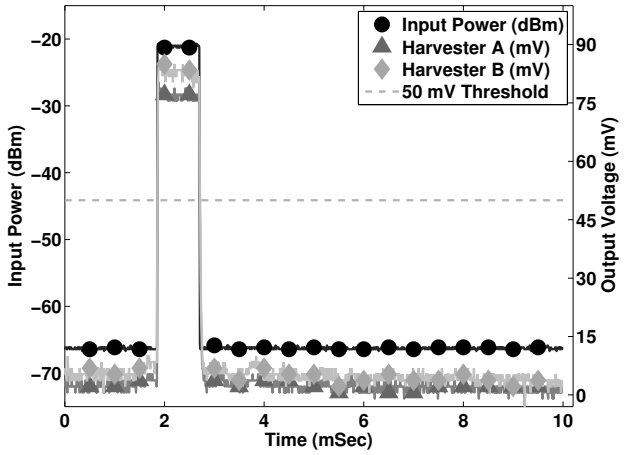


FIGURE 4.11: Measured time-domain response of the diode based harvester driven by an 802.11b/g transmission at -21 dBm

4.5 Optimizing C_X given observed 802.11b/g traffic

The effect of harvester first-stage reservoir capacitor C_X will now be considered. C_X is in parallel with the 5 pF RF bypass capacitor that is always present in the harvester design. The purpose of C_X is to store charge for any subsequent active electronic circuitry. We consider two commonly found power-up threshold voltages:

(1) V_{TH} = 0.8 V, as is typical for CMOS logic in commodity processes, and (2) V_{TH} = 50 mV, as is typical for ultra-low startup voltage boost converters using JFETs [60, 61, 62, 63]. Most prior work in the literature employs one of these two classes of circuitry, although specially doped CMOS transistors, floating gate devices, or SOI transistors may be capable of operation down to voltages approaching $V_{TH} = 50 - 100$ mV as well.

We consider a circuit model shown in Fig. 4.12. The diode output model consists of an open-circuit voltage V_{source} along with a nonlinear source resistance R_{source}. In our work, these model parameters have been extracted from commercial nonlinear device models (Avago Inc), as well as being directly measured *in situ* using the MPP measurement apparatus described above. The load resistance R_{load} includes any leakage currents in C_X as well as the quiescent current of the active circuitry attached to the harvester. We assume in this work that R_{load} is greater than or equal to R_{source}. In our experiments, this condition is enforced using table-lookup MPPT as mentioned above.

The cartoon of Fig. 4.13 shows the effect of the choice of C_X on the ability of the harvester to deliver a voltage above V_{TH}. If C_X is too large, as shown for Harvester B, the active circuitry will never be powered. On the other hand, if C_X is minimized, little energy will be stored in the reservoir C_X and the runtime of the active circuitry will not extend beyond the transmission intervals of the RF source. Harvester A appears intuitively to represent a good choice of C_X.

4.5.1 An expression for usable energy in C_X

We previously defined the usable energy in C_X to be the shaded portion of the curve in Fig. 4.5. We now calculate the usable energy as a function of the known parameters and the unknown capacitance C_X.

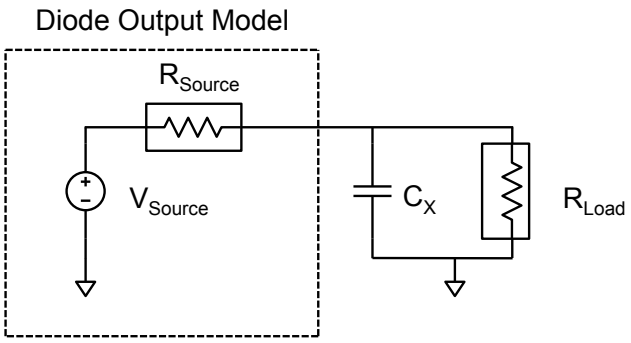


FIGURE 4.12: Circuit model of the harvester including the nonlinear source I-V properties and the presence of C_X

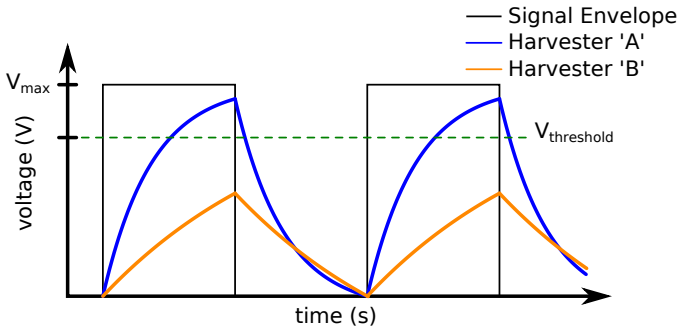


FIGURE 4.13: Cartoon showing the effect of the choice of C_X on stored energy and ability to meet the threshold voltage V_{TH}

The energy E stored on C_X is

$$E = \frac{1}{2}CV^2 \tag{4.1}$$

where C is the capacitance and V is the terminal voltage of C_X. We assume that the energy stored on the capacitor is only usable when the capacitor voltage is above the desired threshold V_{TH}. The usable energy is thus the difference between the stored energy at the end of an RF transmission (at time $t = T_P$) and the stored energy when C_X is charged only to V_{TH}. This is expressed as

$$E_{\text{usable}} = \frac{1}{2}C\left[V_{T_p}^2 - V_{\text{th}}^2\right] \tag{4.2}$$

where

$$V_{T_p} = V_{\text{src}}\left(1 - e^{-T_p/R_L C}\right) \tag{4.3}$$

is the capacitor's terminal voltage at the end of an RF transmission of duration T_p.

4.5.2 Maximizing E_{usable} by choice of C_X given waveform constraints

The usable energy stored on the capacitor can be optimized using a model of the waveform and known harvester characteristics. The MPP curve of the harvester is assumed to be known *a priori*, as in the Matlab table lookup from the measured I-V curve that we have implemented in this proof-of-concept. Based on the expected RF input power of the RF transmission, R_L is constrained to be greater than or equal to R_{src} as measured at the harvester's MPP.

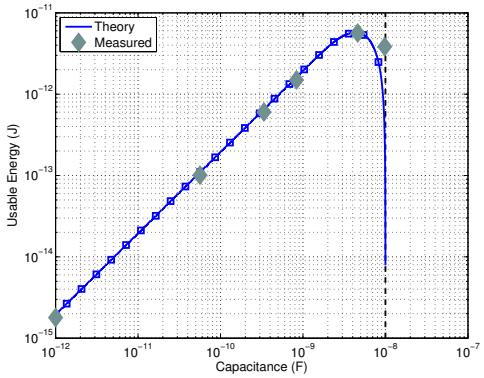
We now substitute to find E_{usable} in terms of C and the known values for R_l, V_{TH}, and T_p

$$E_{\text{usable}} = \frac{1}{2} C {V_{T_p}}^2 \left[e^{-\frac{2T_p}{R_L C}} - 2e^{-\frac{T_p}{R_L C}} + \left(1 - \left(\frac{V_{\text{th}}}{V_{T_p}} \right)^2 \right) \right] \tag{4.4}$$

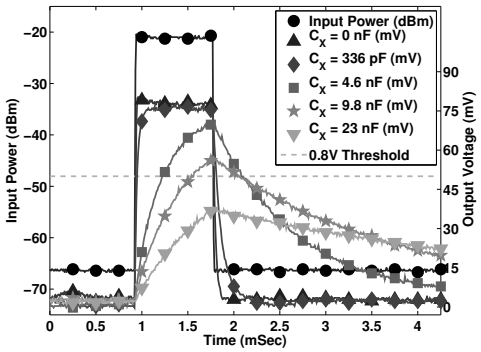
4.5.3 Example choices of C_X given particular 802.11b/g signals

In our benchtop testbed, we have observed that the 802.11b/g traffic always includes at least a series of beacon pulses with $T_p = 1$ ms. Given the sampled RF power $P_{in} = -21$ dBm, the corresponding MPPT load resistance is $R_l = 200$ kΩ. In this configuration, the maximum voltage output from our harvester is 80 mV, which exceeds our V_{TH} requirement of 50 mV. Fig. 4.14(a) shows a plot of Eq. 4.4 given these waveform parameters, while Fig. 4.15(a) shows a similar plot with $P_{\text{in}} = -8$ dBm and $V_{TH} = 0.8$ V. The measured values were obtained from the benchtop testbed by substituting several values of $C_X = \{336 \text{ pF}, 4.6 \text{ nF}, 9.8 \text{ nF}, 23 \text{ nF}, 47 \text{ nF}, 104 \text{ nF}\}$.

Numerical solution of Eq. 4.4 yields optimal values of 4.28 nF for the -21 dBm case, and 26.9 nF for the -8 dBm case. The nearest actual components available for confirmation by measurement were 4.6 nF and 33.9 nF respectively.

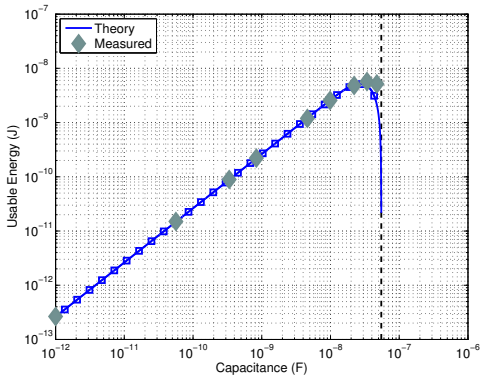


(a) E_{usable} as a function of C_X

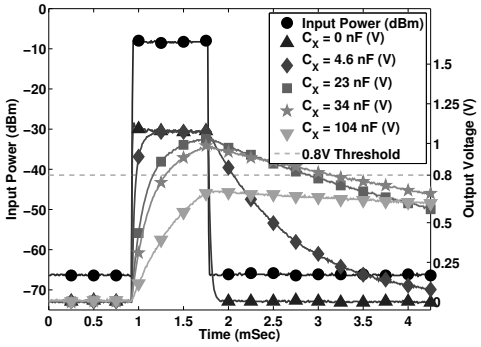


(b) V_{out} as a function of C_X

FIGURE 4.14: $P_{in} = -21$ dBm and $V_{TH} = 50$ mV



(a) E_{usable} as a function of C_X



(b) V_{out} as a function of C_X

FIGURE 4.15: $P_{in} = -8$ dBm and $V_{TH} = 800$ mV

4.5.4 Time domain view of harvester V_{out} vs C_X

Figs. 4.14(b) and 4.15(b) show the measured harvester output voltage V_{out} as a function of C_X in both the low power (-21 dBm) and high power (-8 dBm) cases. The measured behavior aligns well with the cartoon view of Fig. 4.13 in that capacitor values that are too large prevent V_{out} from ever reaching V_{TH}, while values that are too small do not maximize the stored energy.

4.6 Chapter Conclusion

In this chapter we have suggested a new class of RF energy harvesters, which we call "waveform aware harvesters". In contrast to traditional rectenna designs, which are usually designed for high efficiency with continuous wave (CW) signals, waveform aware harvesters are RF to DC converters which are optimized for their performance with non-CW signals. We suggest that waveform aware harvesters may have significant advantages in ambient energy harvesting, where the available RF energy is in the form of communication waveforms that were not designed with harvestability in mind.

We also describe a testbed developed for optimizing harvester performance with realistic Wi-Fi signals. We demonstrate optimized recovery of harvested energy from single Wi-Fi transmission bursts on the order of 1 ms in duration. The proposed approach yields a fairly stable optimum and thus a wide tolerance in the value of reservoir capacitor C_X. Alternative implementations based on switched capacitors, with a circuit implementation analogous to the ultracapacitor switching scheme presented in [66], may offer a good compromise between efficiency gains at the optimal point, and the energy consumed by a dynamic optimization algorithm. While our initial proof-of-concept demonstration has focused on a simple optimization of C_X given bursty 802.11b/g traffic, we believe that many other opportunities may exist for harvester optimization in the presence of communication waveforms.

Chapter 5

A timer-based burst-mode 2.4 GHz energy harvester

5.1 Introduction

The goal of this work is to minimize the required input power to achieve a net positive energy balance between incoming harvested energy and the energy costs of transforming the input signal to a useful voltage level. To reduce the energy requirements of our low voltage boost converter a low power timer is used to trigger the boosting operation. For low input power levels the act of monitoring the input voltage can use more energy than is recovered by the harvester. To extend the range of useful input powers a timer circuit is used to control how often and for how long the boost converter is activated. In this initial proof of concept, a net positive energy balance is achieved at a conducted input power level of -15 dBm at 2.45 GHz, yielding a harvester output voltage of 460mV and a boosted output voltage of 1.8 V.

In order to power the internet of things (IoT) energy harvesting from a variety of sources have been proposed including solar, RF, vibration, thermal, and biological [76, 77, 78]. This work focuses on harvesting from RF energy sources. There are

many examples of RF energy harvesting both from dedicated RF sources [57, 67], and ambient RF sources [58, 54, 65, 79]. Energy can be harvested at low power levels on the order of μWs to 10s of μWs but the output voltage is below what is required for sensor operations. To increase the harvested voltage to a useful level a variety of low power boost converters have been proposed [80, 81] . One of the promising topologies uses a JFET and transformer based circuit. These boost converters have been shown to operate with an input voltage as low as 80 mV [61, 21]. A persistent problem for harvesting from low energy sources is activating a boost converter to bring low voltage inputs up to a useful voltage level, typically around 1 to 3 volts.

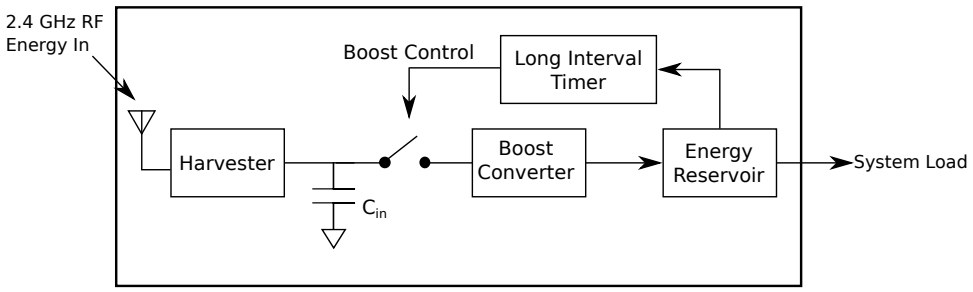
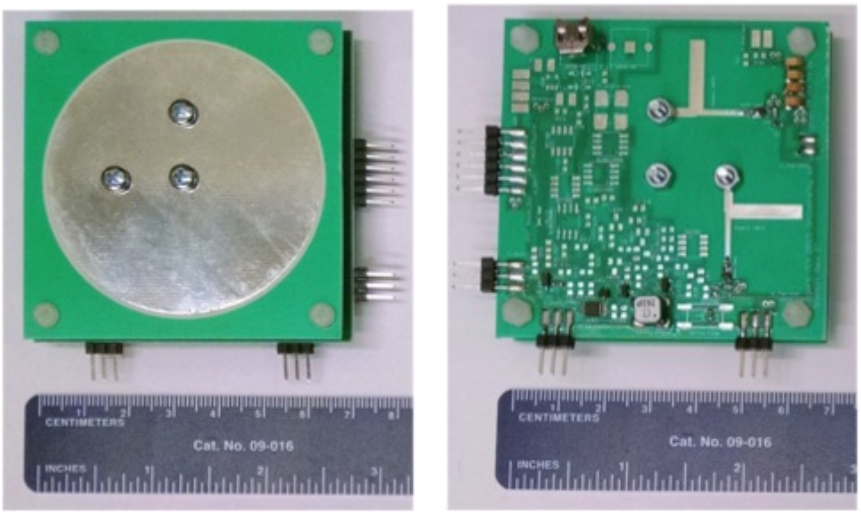


FIGURE 5.1: Timer based harvester system block diagram

The RF energy harvesting system proposed in this chapter is shown in Fig. 5.1. The system consists of a dual polarized circular patch antenna, two RF harvesters, a large input capacitor, a low voltage boost converter, and an output energy reservoir. The energy reservoir can be either a large output capacitor or a battery. In the initial proof of concept a large output capacitor is powered by the boost converter and supplies the timer circuit. For a realistic deployment scenario a battery would be needed to supply power during any extended periods with low available RF power.

The entire system is built on two 7 cm x 7 cm PCBs. The ground plane of the circuits in Fig. 5.2 acts as the ground plane for the dual polarized antenna in Fig. 5.2. An air gap of 5 mm is maintained between the two PCBs by aluminum spacers which also act as the feeding points connecting the antenna to the harvester. The boost



(a) (b)

FIGURE 5.2: (a) Dual Polarized Patch Antenna (b) Integrated RF harvester and timer controlled boost converter.

converter circuit presented in this chapter differs from previous work by introducing a low power timer circuit to activate the low voltage boost converter.

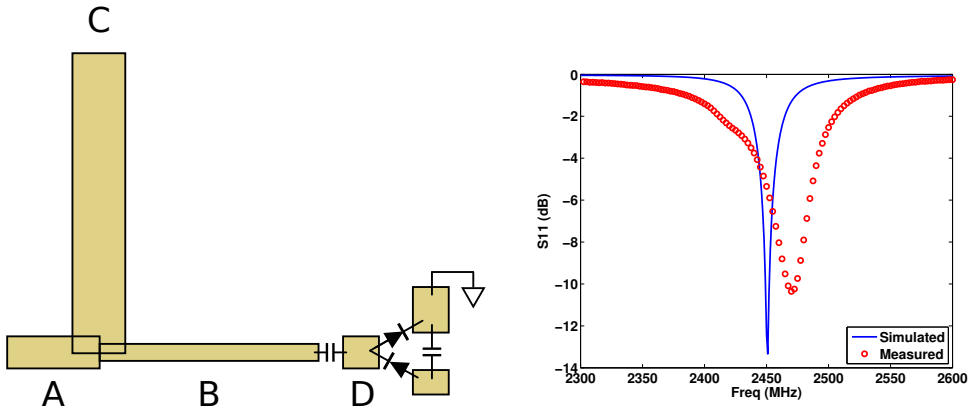
5.2 Related Work

Many examples exist of triggering mechanisms for low power boost converters. An interesting design that tackles the problem of cold starting a low power harvester was done by Ramadass et al. A motion activated switch was used to kick start their system with an input voltage as low as 35 mV [62]. The work in this chapter focuses on extending battery life rather than turning on a system from a zero energy state. Other work has focused on maximizing the harvested energy by dynamically optimizing the trigger for a boost converter [72, 82]. As the power level changes adjustments are made to maximize the input power. Our approach differs from previous work by focusing solely on a single input power. By targeting the minimum input power a low power timer can be used instead of a more energy expensive monitoring circuit. The trade off in lowering the required input power is a decrease

in efficiency at high input powers.

5.3 Diode-based harvester characterization

A single stage rectifier using Avago HSMS286C Schottky diodes converts the input RF energy into a DC output. The Avago HSMS286C diodes were selectedfor their performance at high frequencies and low input power. An open stub matching network was implemented to maximize the power transfer from the dual polarized patch antenna to the diode based harvesters. The design was created in AWR Microwave Office targeting the center of the Wi-Fi frequency band. The matching network was built on a 31 mil Rogers RO4003C substrate. The substrate was chosen for its low loss compared to the more common FR4 substrate material. Measurements of the fabricated matching network were performed on an Agilent N5222A network analyzer. A plot of both the simulated and measured return loss is shown in Fig. 5.3. The frequency that achieves minimum return loss occurs within 10 MHz of the target frequency of 2450 MHz.



(a) (b)

FIGURE 5.3: (a) Matching Network Dimension, wA = 1.81 mm, LA = 5 mm, wB = 0.9 mm, LB = 11.6 mm, wC = 2.9 mm, LC = 16 mm, wD = 1.81 mm, LD = 2 mm. (b) S11 measurements for the simulated and measured matching network

5.4 Timer circuit characterization

A timer based boost converter uses the DC signal from the harvester to produce a 2.2 volt output. The circuit shown in Fig. 5.4 contains a boost converter consisting of a transformer, CoilCraft LPR6235-253PMRB, and a P channel JFET, MMBFJ270. A negative input voltage stored on C_{in} is used by the boost converter to produces a positive voltage across C_{out}. This boosted voltage can be used to charge a battery or a large output capacitor with an eventual goal of driving low power sensors. The boost converter is controlled by a low powered timer circuit, TI TPL5100. The timer controls when the JFET's source is connected to ground. The TI TPL5100 runs off of a 1.8 volt supply and draws a constant current of 30 nA resulting in a power consumption of 54 nW. The timer output drives a PMOS (BSS84W) which drives an N channel FET (FDV301N) and provides the bias to the boost converter JFET. The rds(on) of the N channel FET is a critical parameter for the boost converter operation. When the JFET source is pulled to ground the transition should be as fast as possible and with a low rds(on) to avoid limiting the current flow in the primary coil of the inductor. The rds(on) of the FDV301N FET is 5 Ω.

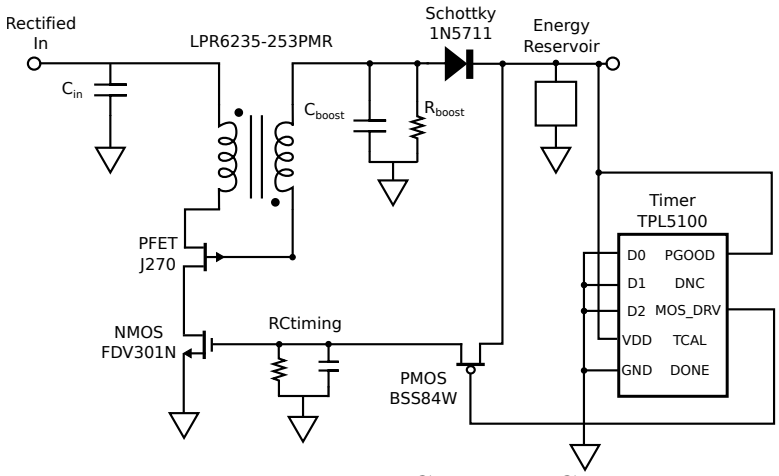


FIGURE 5.4: Boost Converter Circuit

The amount of time the boost converter operates is determined by the resistance

and capacitance of the RC_{timing} components, as seen in Fig. 5.4. The TPL5100 timer produces a square output signal with a 30 ms window. To extend the operating time of the boost converter the RC_{timing} resistor and capacitor stretch the 30 ms window by controlling the discharge rate of the RC_{timing} capacitor. A resistance of 940 MΩ and a capacitance of 4.7 nF were used. This pair allowed the boost converter to run for approximately 1 second, enough time for the input capacitor to be depleted by the boost converter. The RC_{timing} choice impacts the system's operation because the boost converter should only operate for as much time as necessary to deplete charge on C_{in}, the large input capacitor. If the boost converter is turned off too quickly energy is left in the input capacitor that could have contributed to a boosted output. However, if the boost converter is left running for too long any RF energy going into the input capacitor is immediately wasted instead of being allowed to fully charge the input capacitor for the next boosting operation.

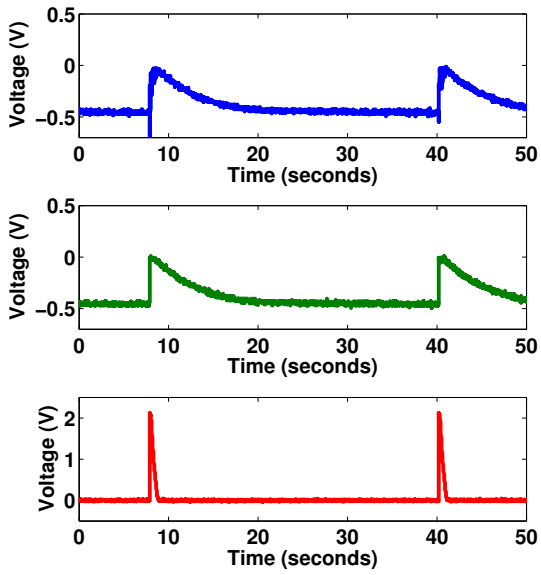


FIGURE 5.5: Operating circuit measured by an Agilent MSO-X-3104A oscilloscope. – JFET source, – JFET drain, – $V_{C_{boost}}$

R_{boost} is used in conjunction with C_{boost} to drain the gate-source voltage of the P

channel JFET. The time it takes for the gate-source voltage to reach the threshold voltage can be configured with the values of RC_{boost}. Keeping the C_{boost} constant at 0.1 uF, R_{boost} can be increased to reduce the duration of wasted energy. If R_{boost} is set too high, the JFET will not be in the saturation when the FDV301N is in saturation. This would result in no oscillations occurring for multiple RC_{timing} pulses. Alternatively, R_{boost} can't be set too low because that would cause the JFET to be in the saturation region before the FDV301N is in saturation. This would increase the duration of wasted energy through the JFET. The optimal R_{boost} value causes the FDV301N and JFET to reach saturation at the same time. Optimizing R_{boost} will assure that the duration of wasted energy is minimized and that the boost converter functions every time there is a pulse from the TPL1500 timer.

Fig. 5.5 shows data collected from the timer circuit when probing the drain of the JFET, source of the JFET, and C_{boost}. The plot shows that when the source of the JFET is pulled to ground, oscillations occur at the drain of the JFET. A boosted output voltage is produced that is used to charge a large output capacitor. The measurement in Fig. 5.5 is for a cabled RF input power of -15 dBm. The timer was set for an interval of 16 seconds. The TI TPL5100 timer can be set to 16, 32, 64,100,128, 256, 512, or 1024 seconds depending on the connections to digital input pins (D0, D1, D2). While the boost converter is off the input capacitor charges to a voltage of -460 mV then is quickly discharged once the boost converter is connected. The boosted output voltage reaches 2.19 volts, enough to charge the output capacitor used to supply the TI TPL5100 timer requirement of 1.8 V.

5.5 System evaluation

To evaluate the boost converter system two separate measurements were performed. The first measurement uses a cabled continuous wave RF input into one harvester to measure the harvester's open circuit voltage. The open circuit voltage is a measure of

the harvester performance independent of the boost converter. This value represents the upper limit of the input voltage to the boost converter for a given input power level.

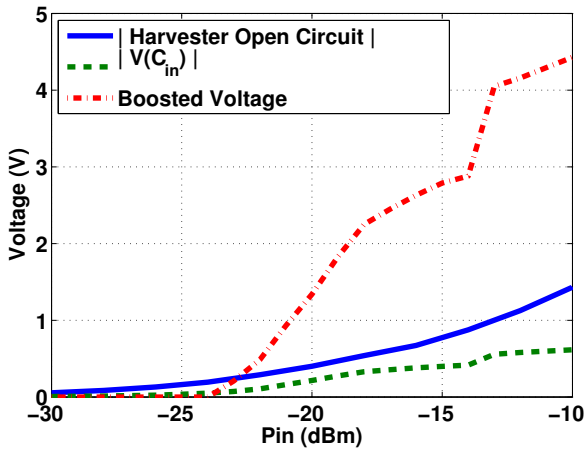


FIGURE 5.6: Timer based boost converter performance vs. input power

The second measurement uses the boost converter in Fig. 5.4 as the output to a single harvester. The 300 μF input capacitor C_{in} and the boosted voltage at the 0.1 μF C_{boost} capacitor were measured with harvester input powers ranging from -30 dBm to -10 dBm. The voltage on C_{in} supplies the input energy to the boost converter. During each timer cycle, the energy on the input capacitor rises until the boost converter is triggered. The values shown in Fig. 5.6 indicates the maximum voltage on C_{in} prior to the boost converter being activated by the timer. The voltage at C_{in} is never as high as the open circuit voltage due to the leakage in the capacitors and the intermittent load presented by the boost converter. The voltage requirement to operate the TPL5100 is reached at -15 dBm. An overhead voltage of 2.19 V is required because of the voltage drop across the 1N5711 diode.

With an input power of -15 dBm a break even point was achieved for harvested energy vs. energy consumed by the timer circuit. An initial voltage of 1.85 volts on the 400 μF capacitor acting as the energy reservoir was used to power the timer

circuit. The harvested energy maintained the energy reservoir voltage of 1.85 volts after 2 hours of testing. Bursts of input energy every 16 seconds made up for the small amount of continuous power being consumed by the timer circuit.

Chapter 6

BLE-Backscatter

6.1 Introduction

Significant challenges remain before the promise of the Internet of Things (IoT) can be realized. Two of the primary challenges limiting the practical deployment of large numbers of IoT sensor nodes include battery lifetime and wireless communication limitations. Many IoT applications are severely energy constrained, either by limited harvestable energy in the environment, or by the desire to maximize the lifetime of batteries given finite energy capacity. Additionally, the need for specialized wireless communication infrastructure (such as Zigbee / 802.15.4 Internet gateways, or even extra WiFi access points to achieve good coverage) creates a cost and maintenance barrier impeding wider adoption of IoT sensor nodes.

Modulated backscatter communication (MBS) relies on the time varying reflection of an externally generated carrier source in the environment. The backscatter device need not bias any active devices for gain at the carrier frequency, which permits the dramatic savings in operating power compared to a conventional transmitter employing a power-hungry frequency synthesizer. In the RFID case, a continuous

wave (CW) carrier is supplied by the RFID reader that is powering up the tags. We have previously demonstrated that MBS can be used to generate ASK, FSK, PSK, and QAM modulated signals at data rates of up to 96 Mbps with orders of magnitude savings in node energy cost per bit (pJ/bit) compared with conventional transmitters (> 10 nJ/bit) [83, 4]. In this work we consider a special case where PSK backscatter modulation is used to generate a subcarrier in one or more Bluetooth 4.0 low energy (BLE) channels. The subcarrier is then FSK modulated with the desired data. The resulting backscatter signal thus has a band-pass component which is in-channel from the perspective of the BLE receiver. This approach yields a BLE-Backscatter signal which can be demodulated and passed up an existing BLE stack without any modifications whatsoever to hardware, firmware, or software. This approach is of interest because Bluetooth 4.0 Low Energy (BLE) compatible chipsets are widely deployed in essentially all smart phones, tablets, and PC's from major manufacturers including Apple, Samsung, etc. Shipments of BLE-enabled devices have recently exceeded over a billion units per year [45, 84].

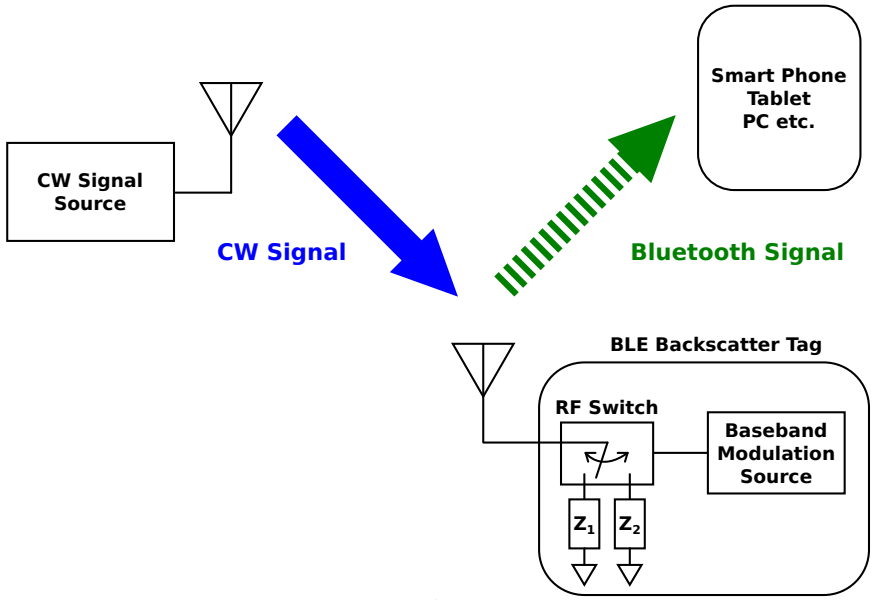


FIGURE 6.1: BLE-Backscatter system concept

In this work, an expanded version of [3], we demonstrate MBS devices that generate signals that can be received by unmodified BLE devices. From the point of view of the BLE receivers, the MBS signals are indistinguishable from conventional BLE advertising transmissions. The key insight is that backscatter modulation can be considered as a mixing process, where an incident carrier source is mixed at a backscatter modulator with a baseband or subcarrier signal generated locally in the backscatter device. We have previously shown in [3] that both fundamental mode and harmonic mode mixing can be used to create BLE compatible signals.

In our prior work we used laboratory equipment including an arbitrary waveform generator to generate the backscatter signal. In this work, we present a stand-alone, low power (sub-1 mW) implementation of the BLE-Backscatter concept with an MSP430 based tag powered by a CR2032 lithium watch battery. The stand alone implementation eliminates the need for laboratory instruments and points the way to a practical application. We demonstrate reception of the backscattered BLE messages with two unmodified BLE devices, an Apple iPad mini and a generic PC equipped with a Nordic Semiconductor nRF51882 BLE chipset. Each device successfully demodulates and accepts the advertising messages, passing them up their Bluetooth stacks without any modifications whatsoever. Successful reception is shown at a range of 13 meters using a +23 dBm EIRP fixed frequency source.

The structure of this chapter is as follows: In Section 6.2 we review related work in wireless sensors for IoT applications. Section 6.3 describes the key features of the BLE specification that enable backscatter devices to be interoperable with conventional Bluetooth devices. In Section 6.4 we consider backscatter modulation as a mixing process and show how a carefully constructed baseband or subcarrier modulation can produce band-pass signals compatible with the conventional BLE channel scheme. In Section 6.5 we describe the stand-alone BLE-Backscatter tag. Section 6.6 presents our experimental results in over-the-air testing, and summarizes

the energy advantage of the BLE-Backscatter concept. Finally, Section 6.7 presents our concluding thoughts on this concept.

6.2 Related Work

One early vision for the nascent Internet of Things (IoT) is the Berkeley "Smart Dust" of the early 2000s [85]. The initial smart dust mote concept included a solar cell for energy harvesting, a variety of sensors, and an optical backscatter communication link using a modulated MEMS mirror to communicate by selectively reflecting laser energy from an external source. The development of battery-free UHF RFID tags using the EPC Generation 2 standard also occurred during this period, using less exotic standard-CMOS compatible technologies of RF energy harvesting and RF backscatter communication. The availability of Generation 2 RFID tags and readers led to the development of the popular wireless identification and sensing platform (WiSP) family of devices [33]. These low power, microcontroller-based RFID tags use RF energy harvesting and backscatter communication compatible with the Generation 2 RFID standard. The programmability of the general purpose microcontroller on the WiSP has enabled a variety of battery-free sensing demonstrations including capacitive touch sensors, acoustic sensors, and battery free cameras [34, 35].

One drawback of Generation 2 RFID devices, including the WiSP platform, is the reliance on specialized RFID reader hardware to receive data from the tags or WiSP sensors. While the Generation 2 RFID technology has continuously grown in industrial importance, it remains largely confined to commercial and industrial applications and is not yet widely available in the consumer space. In contrast, the Bluetooth 4.0 Low Energy (BLE) standard has experienced explosive growth in both consumer and industrial applications, with billions of BLE devices now deployed each year. Essentially all smart phones and tablets now support BLE, so it has become a ready-made platform for communication with sensor devices. A variety of use

cases have been suggested for BLE including industrial applications [86], vehicular applications [87], in smart agriculture [88, 89], in smart homes [90], and for a range of medical applications [91, 92, 93, 94, 95].

One challenge in leveraging BLE for sensor data uplink is the need for a battery or other energy source to power the BLE devices. Batteries suffer from the significant drawback of limited capacity and thus limited lifetime; they thus create a long tail of maintenance that must be considered when deploying large numbers of sensors, particularly in inaccessible places. An eventual objective of this work is to combine energy harvesting with backscatter communication to eliminate the need for batteries, yet retain compatibility with BLE receivers. In areas where ambient energy in the 2.4 GHz band is available, the same 2.4 GHz signal that provides power to the BLE-Backscatter device could be used to provide the communication carrier. Recent work including [96, 97, 79, 22, 98, 99] has served to quantify the available energy in typical indoor and outdoor environments, and demonstrated a variety of strategies for harvesting that energy.

In addition to the use of specialized carrier emitters, for example specialized readers in the RFID case, it has recently been shown that "signals of opportunity" such as digital TV broadcast signals [43] and Wi-Fi [14] signals can be used as carriers for backscatter communication. In [43] and [14], the MBS signals were modulated in a non-standard manner that required custom firmware and a custom software stack to receive the backscattered data. In this work we demonstrate an alternative approach that yields BLE-Backscatter signals that are indistinguishable from ordinary BLE beacon transmissions from the BLE receiver's perspective; no modifications whatsoever to hardware, firmware, or software are needed. Thus the approach presented here enables billions of existing BLE devices to serve as a ready-made IoT infrastructure.

6.3 Relevant aspects of the Bluetooth 4.0 Low Energy (BLE) standard

BLE is an ideal candidate for demonstrating modulated backscatter compatibility with conventional devices because billions of existing smartphones, tablets, and other devices are BLE enabled, and the physical layer is relatively simple. One mode of operation supported by the BLE standard is a beacon mode, where low power, transmit-only sensors or devices periodically transmit in one of three dedicated "advertising channels" set aside for this purpose. BLE compatible receiving devices must periodically listen in each of the three advertising channels in turn to receive broadcast advertising packets from the beacon devices. One example application leveraging this mode of operation is Apple's iBeacon, which provides location awareness to their iOS devices [15].

In this work, we leverage three key BLE features to achieve a similar functionality to iBeacon using a backscatter based device. First, sensor ID and data may be broadcast in advertising packets, without requiring acknowledgements. Second, the three advertising channels defined in the BLE spec use a fixed modulation scheme, Gaussian-shaped binary FSK at 1 Mbps in three fixed frequency channels centered on 2402 MHz, 2426 MHz, and 2480 MHz. Third, every BLE receiver must listen for incoming advertising packets across all three advertising channels, so reception of advertising packets on any one channel is sufficient for the message to be received with probabilistic delivery.

6.3.1 BLE Frequency Plan

There are two different types of channels in the BLE frequency plan: *advertising channels* used for unidirectional (broadcast) communication, including device discovery and sensor beacons, and *data channels* used in bidirectional communication. Three advertising channels, shown in blue in Fig. 6.2, are spread out over the 2.4 GHz

ISM band to mitigate jamming or fading. Per the BLE specification, the advertising channels serve to advertise services and establish data links, and they also provide for a broadcast sensor data uplink capability, as is exploited by e.g. Apple's iBeacon devices.

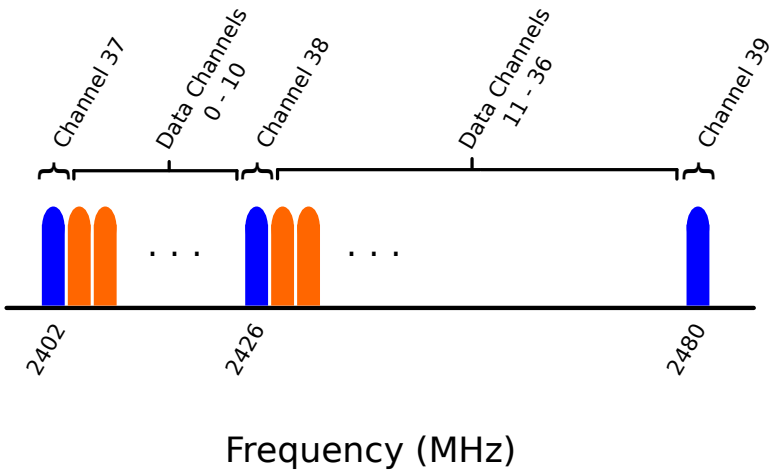


FIGURE 6.2: BLE frequency plan showing advertising (blue) and data channels (orange)

6.3.2 BLE channel layout

Each of the 40 BLE channels occupies a 2 MHz bandwidth specified by the channel center frequency, F_c. The modulation scheme is Gaussian-shaped binary frequency shift keying (FSK) at a data rate of 1 Mbps. A positive frequency deviation above the channel center frequency corresponds to a "1" bit and a negative frequency deviation corresponds to a "0" bit. The frequency deviations must be greater than 185 kHz as shown in the example channel layout in Fig. 6.3. A Gaussian filter is used to smooth the data transitions.

6.3.3 BLE Advertising Packet Structure

While many different types of packet structures are defined in the BLE specification, this work is focused solely on BLE advertising packets. One popular advertisement

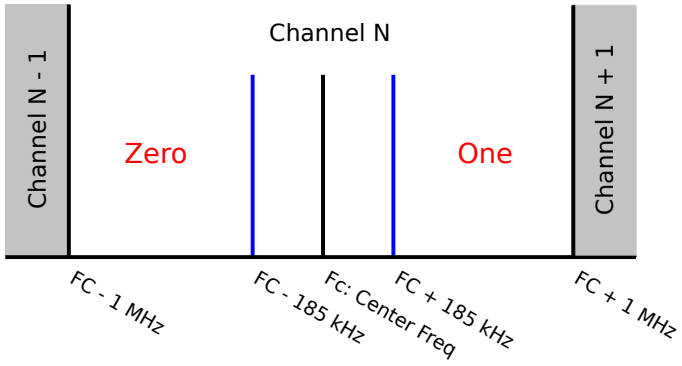


FIGURE 6.3: Channel layout of a single 2 MHz wide BLE channel.

packet structure is the Apple iBeacon which has a major and minor ID string, unique identifier (UUID), and an Apple, Inc. company ID [15], although the approach presented here is not limited to the iBeacon standard and can be used with any advertising packet format.

Each advertising packet consists of four parts as shown in Fig. 6.4. The first 8 bits comprise a preamble, followed by a 32 bit access address, then a variable length payload data unit (PDU), and finally a 24 bit CRC. The PDU can vary from 16 to 312 bits and is the portion of the packet that contains node specific data. For our proof of concept BLE-Backscatter devices, we transmit 232-bit packets containing recognizable English device names, such as “Alice” and “Bob”. Per the BLE specification, each packet must be uniquely encoded for transmission on a specific channel. To achieve this, we employed a data whitening linear feedback shift register (LFSR), with an initial register value based on the specific channel number. For example, the “Alice” packet is formatted for transmission on channel 37 and the “Bob” packet on channel 38.

6.4 Spectral engineering for MBS-BLE compatibility

In most backscatter communication systems, the functions of carrier generation and modulation are partitioned between two separate devices (for example, a reader and

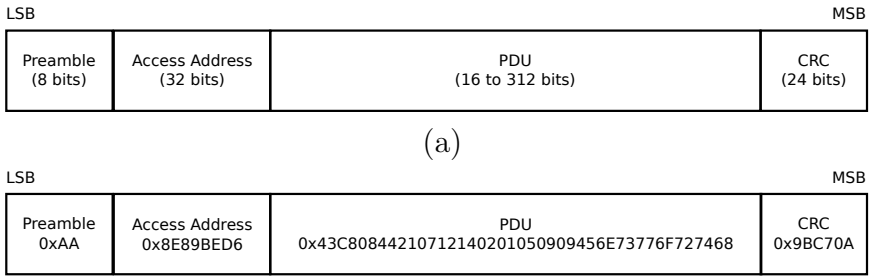


FIGURE 6.4: (a) BLE packet format (b) example packet bit string

a tag in the RFID case). This partition enables the power burden of generating a carrier signal to be offloaded to an energy rich device, allowing the backscatter tag or sensor to consume much less power than a conventional transmitter-based device. In the BLE-Backscatter case, the tag or sensor makes use of a carrier at a known frequency to generate band-pass signal components in the fixed advertising channels.

6.4.1 MBS as a Mixing Process

A key insight of this work is to consider the backscatter modulator as a 2-port switching mixer, mixing the externally generated carrier with a locally generated subcarrier, and where at least one of the mixing products is in-band with respect to the BLE channel scheme. To create a BLE compatible message, we modulate the externally supplied carrier with a locally-generated offset subcarrier that drives a backscatter modulator between two impedance states (in our case, open and short, producing a double sideband PSK signal). The offset subcarrier is in turn FSK modulated by a baseband signal at 1 Mbps to match the BLE specification. The resulting spectrum thus contains two band-pass signals that are each compatible with the BLE specification. We have previously shown [3] that a single CW signal along with a combination of fundamental and harmonic mode subcarriers can achieve transmission in all three BLE advertising channels.

The most straightforward method of creating the MBS signal is to use a fixed CW

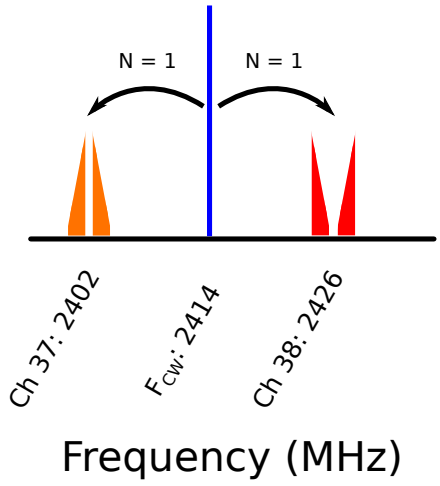


FIGURE 6.5: Frequency plan serving channels 37 and 38 using $N = 1$ with a fixed $F_{cw} = 2414$ MHz

carrier frequency, F_{cw}, and the fundamental mode of the offset subcarrier. The BLE receiver is expecting a binary FSK signal centered at the channel's center frequency F_c with a deviation $\delta f_{BLE} \geqslant \pm 185$ kHz. We can accomplish this by introducing an offset subcarrier, f_{sc}, that is itself FSK modulated with the same deviation, $\delta f_{sc} = \delta f_{BLE}$. When a CW carrier is backscatter modulated with the offset subcarrier, the resulting double sideband spectrum contains the following components:

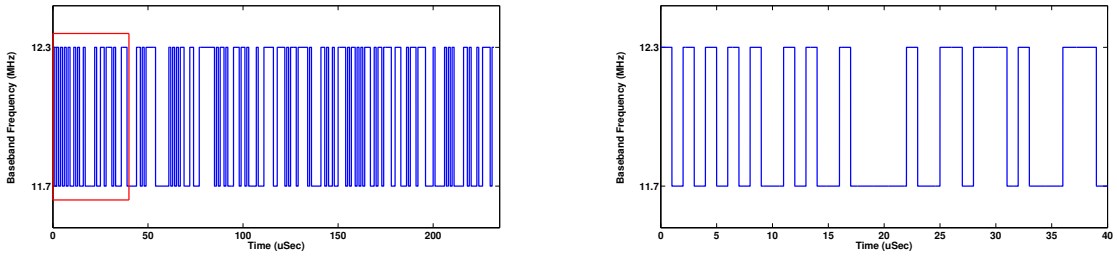
$$M \cdot F_{cw} \pm N \cdot (f_{sc} \pm \delta f_{sc}) \tag{6.1}$$

where M is the carrier harmonic number and N is the subcarrier harmonic number. In this chapter we use the fundamental mode with M and N equal to 1. Either the upper or the lower sideband spectrum (USB/LSB) may be used to reach the desired BLE channel frequency. To reach multiple advertising channels while minimizing the subcarrier frequency one can choose to use both the LSB and USB spectra, with a carrier frequency centered e.g. between BLE channels 37 and 38 at $F_{cw} = 2414$ MHz as shown in Fig. 6.5. The necessary subcarrier frequencies are thus

$$f_{sc,0} = 12 - \delta f_{sc} = 11.7 \text{ MHz}$$

$$f_{sc,1} = 12 + \delta f_{sc} = 12.3 \text{ MHz}$$

With this frequency plan the USB is used to reach channel 38 and the LSB is used to reach channel 37 as shown in Fig. 6.5. For the USB component, a positive subcarrier deviation, δf_{sc}, results in a "1" being recorded at the receiver and a negative subcarrier deviation results in a "0". However, for the LSB component a positive subcarrier deviation now results in a negative frequency deviation as observed by the receiver at channel 37. To account for this the data bits of BLE messages intended for channel 37 must be inverted prior to transmission.



(a) (b)

FIGURE 6.6: (a) Entire "Bob" packet (b) Zoom of preamble and access address regions

Fig. 6.6 shows an example of how packets were created for one of the messages used in this chapter. The BLE message has a length of 232 bits and with a data rate is 1 Mbps resulting in a transmit time of 232 μS. To transmit a "1" a baseband frequency of 12.3 MHz is generated and to transmit a "0" a baseband frequency of 11.7 MHz is generated. Fig. 6.6 b shows the first 40 μS of a BLE packet consisting of the preamble and access address.

6.4.2 Interference due to unwanted mixing products

In addition to the desired mixing products there are unwanted frequency components generated by modulated backscatter. This is true of conventional UHF RFID tags as well as the BLE Backscatter devices presented here. To date, regulatory bodies such as the US FCC have allowed backscatter devices to radiate unwanted frequency components as long as the out-of-band emissions comply with the applicable incidental radiator regulations, for example as specified by FCC regulations Part 15.247. To date we haven't observed any interference between our MBS BLE tags and other nearby Wi-Fi or BLE devices, but a careful characterization of potential interference represents an important area for future work.

6.5 Standalone BLE Backscatter Tag Implementation

In prior work [3], we presented an early experiment using a bench top arbitrary waveform generator to produce the required subcarrier signals. In this work we present a standalone, battery-operated low power (sub-mW) BLE Backscatter tag that doesn't rely on test equipment.

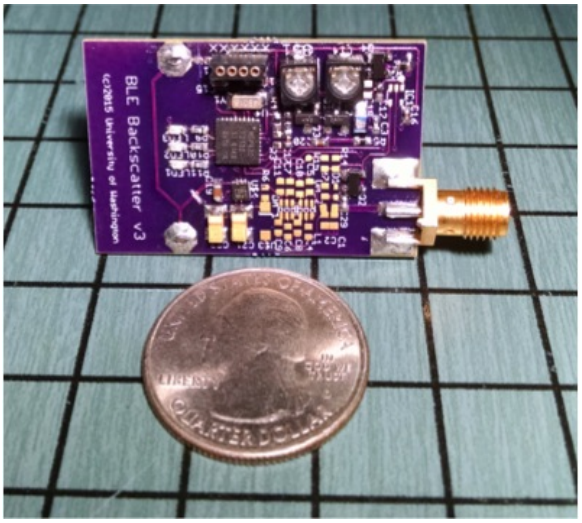


FIGURE 6.7: Stand alone board level prototype

The stand-alone BLE Backscatter tag implementation was designed for low power consumption by using a custom designed analog clock generator to generate the required subcarrier. A block diagram of the tag is outlined in Fig. 6.8 and a photo of the tag is shown in Fig. 6.7. This tag consists of a TI MSP430F2132 microcontroller controlling an analog oscillator which in turn drives an Analog Devices ADG918 RF switch. The analog oscillator is continuous-phase frequency modulated at 1 Mbps with a frequency deviation of $\pm$300 kHz. The tag is powered by a CR2032 lithium coin cell battery regulated down to 2.5 V by an LT3008 linear regulator. Between transmissions, the analog oscillator and RF switch are disabled and the MSP430 enters sleep mode, reducing current consumption to $\approx$ 1 μA. To reduce the power consumption during active mode, the microcontroller clock rate was set to the lowest possible frequency of 1 MHz. Hardware serial clocking on the MSP430 permits the processor to clock out BLE data bits at the required rate of 1 Mbps (one bit per clock cycle).

Fig. 6.8 presents the schematic of the subcarrier oscillator. It is a cross-coupled LC oscillator with a fixed inductor and a parallel combination of a fixed capacitance (150pF // C_{tune1}) and a switched additional capacitor C_{tune2}. The frequency select line controls which frequency the oscillator will generate. A first subcarrier frequency is generated when the BF1105 switching FET is open and a second subcarrier frequency is generated when the switching FET is closed and C_{tune2} increases the total capacitance. The frequency select signal is driven by the MSP430's hardware serial peripheral. In the initial prototype, 4 - 25 pF variable capacitors are used for C_{tune1} and C_{tune2} to account for component variation and allow fine tuning of the subcarrier frequencies. In a future single-chip implementation, a capacitor array would likely be considered to implement these capacitances to permit digital tuning. Adjusting the frequency with a switched capacitor allows for a phase continuous transition between the two subcarrier frequencies, which is important for proper reception at the BLE

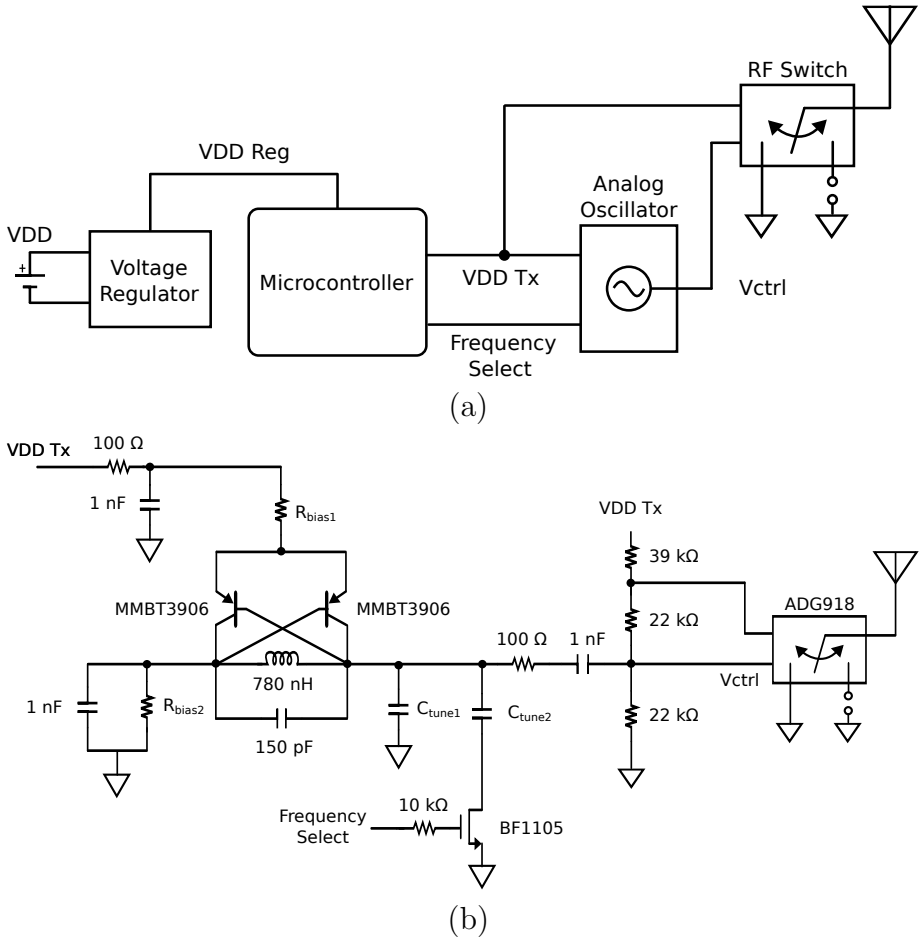


FIGURE 6.8: (a) Block Diagram of BLE-backscatter tag (b) Circuit diagram of analog oscillator and modulating RF switch

receiver.

An engineering tradeoff in this circuit is the balance between biasing for low current consumption and achieving an acceptable voltage swing to drive the modulating switch. The bias resistors, R_{bias1} and R_{bias2} set the DC operating point and limit the current drawn by the oscillator. In the prototype tag the bias point was set with $R_{bias1} = 2$ kΩ and $R_{bias2} = 4.7$ kΩ given our choice of the ADG918 RF switch which has an internal LVCMOS switching threshold.

The BLE Backscatter tag sends alternating messages designed for BLE advertising channels 37 and 38. The message sent on channel 37 contains the device name

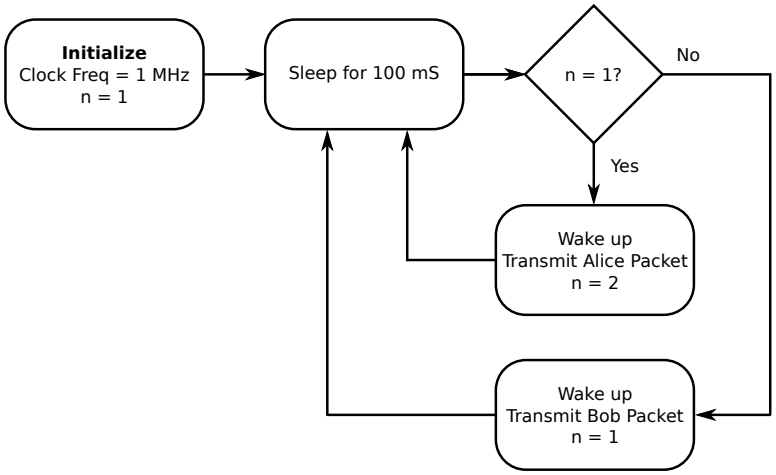


FIGURE 6.9: Stand alone board state machine

"Alice" and the message sent on channel 38 contains device name "Bob". As shown in Fig. 6.9 after initialization the tag alternates between "Alice" and "Bob" messages with a 100 mS deep sleep period between messages. This tag operates with the frequency plan outlined in Fig. 6.5 where an externally supplied CW carrier frequency of 2414 MHz is provided. The lower sideband (LSB) targets channel 37 and has subcarrier frequencies

$$f_{sc,0,LSB} = 12 + 0.3 = 12.3 \text{ MHz}$$

$$f_{sc,1,LSB} = 12 - 0.3 = 11.7 \text{ MHz}$$

and the upper sideband (USB) targets channel 38 and has subcarrier frequencies

$$f_{sc,0,USB} = 12 - 0.3 = 11.7 \text{ MHz}$$

$$f_{sc,1,USB} = 12 + 0.3 = 12.3 \text{ MHz}$$

To set the tuning capacitors to achieve the desired frequencies a cabled backscatter setup was used to avoid capacitively loading the oscillator circuit by directly probing the V_{ctrl} signal. Fig. 6.10 shows the implemented backscatter frequencies captured on an Agilent N9320B spectrum analyzer.

The tag's firmware consists of a loop. It enters a sleep mode for 100 ms, the minimum inter-packet interval described in the Bluetooth V4 specification [45], then

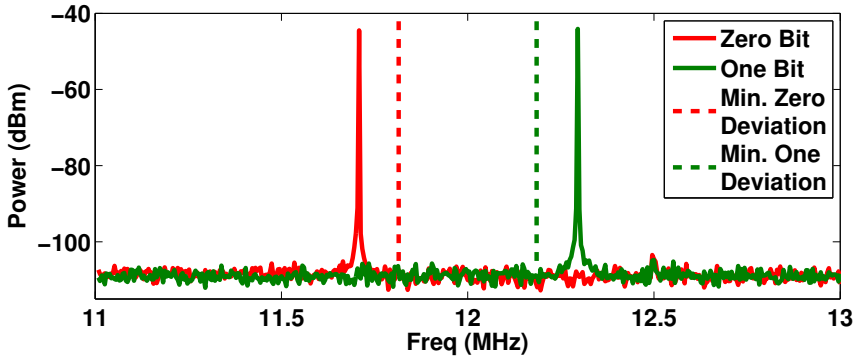


FIGURE 6.10: Subcarrier frequencies observed with a spectrum analyzer

wakes up and alternates sending either an Alice or a Bob packet. Fig. 6.11 shows a time domain capture of the VDD Tx, Frequency Select, and V_{ctrl} signals during a single packet transmission. The active-mode duration is 270 μs to account for wake up, transmission of a 232 bit message, and returning to a sleep mode.

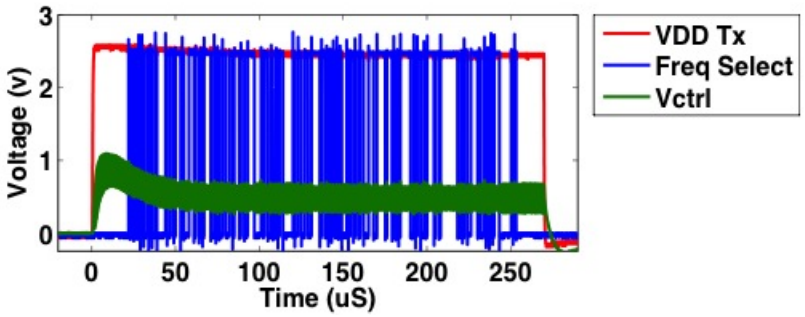


FIGURE 6.11: Oscilloscope capture showing key signals in the BLE-backscatter tag as the tag wakes up, transmits a single packets, and enters sleep mode.

6.6 Experimental Results

6.6.1 Link Budget

A link budget based on the approach of [100] was calculated to estimate the operating range of the BLE Backscatter tag. The BLE Backscatter system is similar to a bistatic radar setup where the CW source and BLE receiver are physically separated. The received power at the BLE receiver is calculated as the product of two parts.

Referring to the geometry of Fig. 6.13, the backscattered power available from the tag is

$$P_{tag} = \frac{P_t G_t \Delta\sigma}{4\pi D_1^2} \tag{6.2}$$

where D_1 is the distance from the CW signal source to the tag, P_t and G_t are the CW source output power and gain of the transmitting antenna respectively, and $\Delta\sigma$ is the differential radar cross section (RCS) [101, 102, 83] given by

$$\Delta\sigma = \frac{\lambda^2}{4\pi} G_N^2 \left|\Gamma_1^* - \Gamma_2^*\right|^2 \tag{6.3}$$

where G_N is the antenna gain of the node (tag) and Γ^* is the conjugate match reflection coefficient

$$\Gamma^* = \frac{Z_a^* - Z_L}{Z_a + Z_L} \tag{6.4}$$

for a resonant antenna impedance Z_a and the complex load impedance Z_L.

The power received at the BLE receiver (e.g. a smartphone) is

$$P_R = \frac{P_{tag} G_r \lambda^2}{(4\pi)^2 D_2^2} \tag{6.5}$$

where G_r is the gain of the receiver's antenna and D_2 is the distance from the tag to the BLE receiver.

Combining Equations 6.5 and 6.3 gives the backscattered power at the BLE receiver, assuming that antenna gains and transponder RCS are in the preferred orientation

$$P_R = \frac{P_t G_t \Delta\sigma G_r \lambda^2}{(4\pi)^3 D_1^2 D_2^2} \tag{6.6}$$

Table 6.1: Parameters for link budget calculation

λ	0.124 meters
P_t	+20.9 dBm
G_t	2.1 dBi
G_N	2.1 dBi
G_r	0 dBi (estimated)
Z_a	50 + j 0 Ω
Z_{L1}	76 - j 74 Ω
Z_{L2}	78 + j 93 Ω

Parameters for the link budget calculations are shown in Table 6.1. The CW source and tag antennas are dipole whip antennas with 2.1 dBi gain. We have assumed that the gain of the BLE antenna in the iPad or smart phone is approximately 0 dBi. Values for Z_{L1} and Z_{L2} were measured over the 2400 MHz to 2483 MHz band with modulating RF switch control voltages of 0.4 and 0.5 V, representing either side of the measured logic threshold of the ADG918 switch. Measurements shown in Fig. 6.12 were performed with an Agilent N5222A PNA network analyzer at the SMA port of the stand alone board. The values of Z_{L1} and Z_{L2} at 2414 MHz were used in our link budget calculation since that is the mid point between BLE advertising channels 37 and 38.

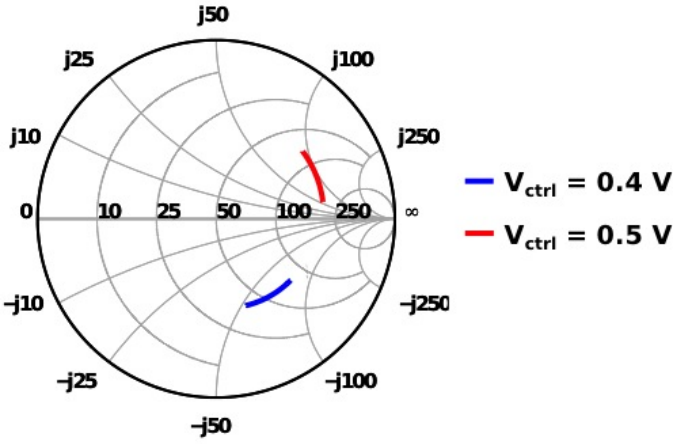


FIGURE 6.12: Measured S_{11} of ADG918 over 2400-2480 MHz, V_{ctrl} = 0.4 V and 0.5 V.

6.6.2 Over-the-air (OTA) test setup

To validate the link budget analysis in an indoor environment (a hallway in our building), we temporarily programmed a BLE Backscatter tag to backscatter at a constant subcarrier frequency. As shown in Figs. 6.13 and 6.14 we recorded the received power with an Agilent N9320B spectrum analyzer as a function of distances D_1 and D_2, with the CW carrier source, BLE Backscatter tag, and receiving BLE device positioned on moveable plastic carts. Dipole whip antennas are used for the CW carrier source and BLE tag and are positioned at the edge of the plastic carts with a horizontal polarization. The CW carrier is generated by an Agilent N5181A signal generator and amplified with a Mini Circuits ZRL-3500+ RF amplifier to provide a transmit power of $P_t = +20.9$ dBm. The BLE Backscatter tag is placed between the carrier source and the receiving device, either an Apple iPad mini or a spectrum analyzer depending on the experiment. The BLE Backscatter tag was moved in ≈ 1 meter increments with the total distance between the CW source and receiver fixed at ≈ 13 m. At each step the received power at the spectrum analyzer was recorded.

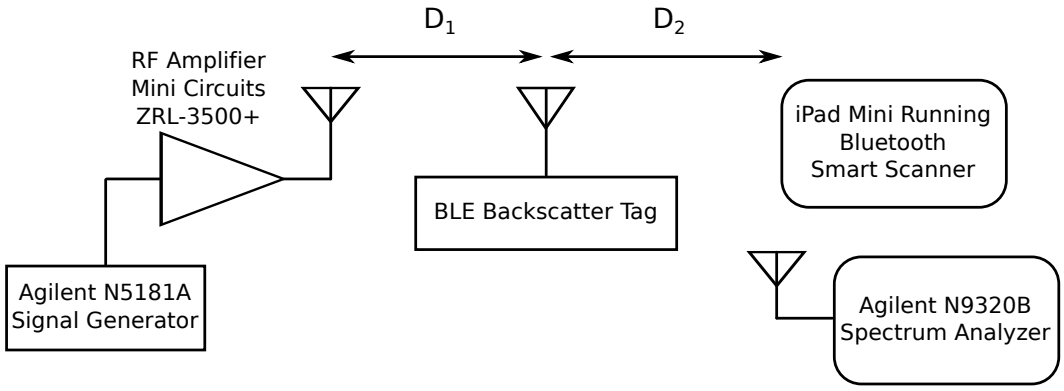


FIGURE 6.13: OTA test setup diagram

The received power at a variety of distances D_1 is displayed with red squares in Fig. 6.15 and the estimated received power from Eq. 6.6 is plotted with a solid

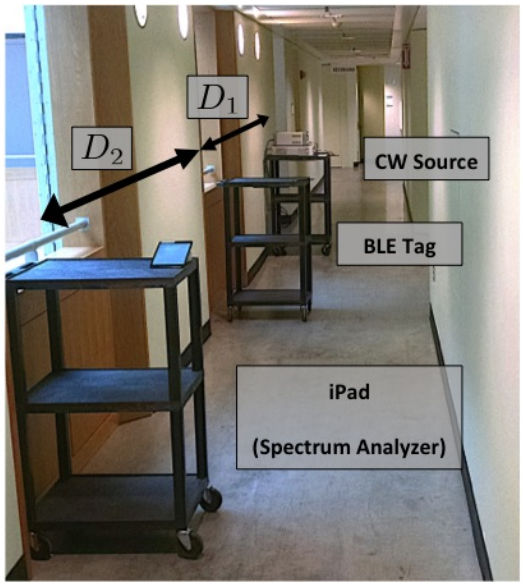


FIGURE 6.14: Photo of OTA test setup

blue line, and the manufacturer's specified receiver sensitivity of a commercial BLE device, Nordic Semiconductor nRF51822, is plotted with a dashed black line. The receiver sensitivity indicates the power level required for a bit error rate $< 0.1\%$.The measured received power is close to what we predicted based on the link budget analysis, modulo the effect of multipath propagation in the hallway. The estimated power follows a symmetrical bathtub curve where the received power is maximized when the BLE tag is close to either the CW source or the BLE receiver. We attribute the discrepancy between the calculated and measured results to multipath reflections in the hallway environment.

Following the spectrum analyzer measurements, the backscattered "Alice" and "Bob" messages were received at every measured location within the 13 m range, with the iPad mini and a Nordic Semiconductor nRF51882-based USB dongle acting as a receiver. Fig. 6.16 presents a screen shot from the iPad mini running a BLE scanner app showing the device names "Alice" and "Bob" for the received BLE packets as expected. We found that the RSSI values reported by the iPad BLE Scanner app are

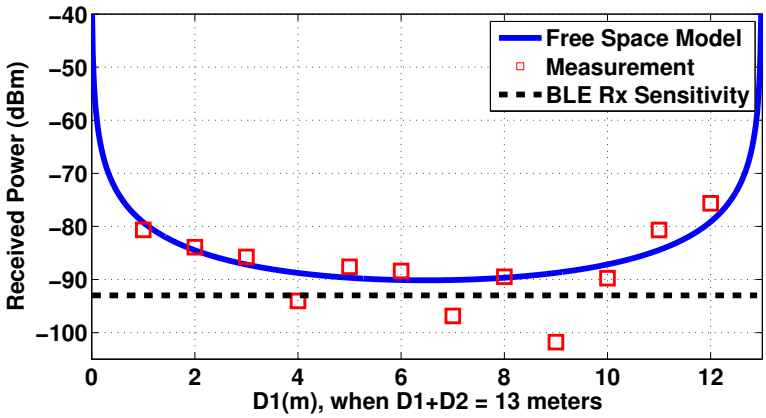


FIGURE 6.15: OTA signal strength from the BLE Backscatter tag

significantly different than those measured by the spectrum analyzer. This could be attributed to a combination of poor calibration of the iPad's receiver chipset or the iPad's BLE stack, and/or the unknown radiation pattern of the Bluetooth antenna inside the iPad. We feel that the spectrum analyzer measurements are more reliable than those reported by the BLE Scanner app.

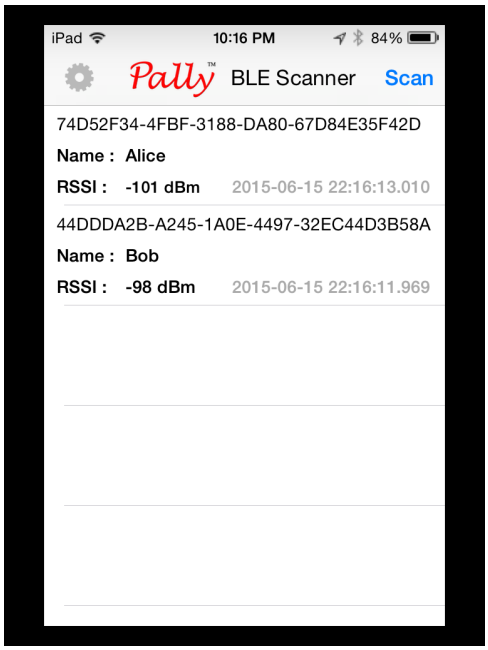


FIGURE 6.16: iPad screenshot showing successful reception of "Alice" and "Bob" messages

6.6.3 Energy Savings of BLE-Backscatter vs Conventional BLE

A primary reason for decoupling the carrier generation and baseband modulation in the BLE-Backscatter concept is to reduce the energy requirements of the tags. A necessary energy expenditure when generating an RF signal are the switching losses associated with charging and discharging capacitors. The energy consumed by charging and discharging a capacitor is:

$$E = \frac{cV^2fT}{2} \tag{6.7}$$

where c is the capacitance, V is the voltage, f is the switching frequency, and T is the time during which the varying voltage is present. The switching energy is proportional to the operating frequency meaning that a lower operating frequency is desirable for an energy poor device like a sensor node. Lets take for example the ADG918 RF switch used in this work. The control input capacitance for this switch is $\approx$ 2 pF, the operating voltage swing is 0.1 V, and the switching rate is around 12 MHz. The BLE data rate is 1 Mbps so the FET must be switched for 1 μsec per transmitted bit. The energy used in charging and discharging the input control capacitance is thus 0.12 pJ/bit, over two orders of magnitude less than if the signal was at the carrier frequency of 2414 MHz.

Table 6.2 compares the measured energy per bit of the BLE-Backscatter tag to the datasheet-supplied energy consumption of the frequency synthesizer and transmitter sections only (not counting microprocessor or baseband energy consumption) of three widely used conventional BLE chipsets: the Nordic Semiconductor nRF51822, the Texas Instruments CC2540F128, and the Dialog Semiconductor DA14580. The calculated energy per bit is based on a 232-bit BLE advertising packet. As shown in Table 6.2, the prototype BLE-Backscatter tag achieves over 6X reduction in energy per bit transmitted, compared to state-of-the-art conventional BLE transmitters.

Table 6.2: Energy / bit comparison

Radio Type	**Device Name**	**TX Active Current**	**Voltage**	**232-bit pkt Energy/bit**
Conventional	Nordic Semi. nRF51822	6.3 mA	3 V	18.9 nJ/bit
Conventional	TI CC2540F128	18.6 mA	3 V	55.8 nJ/bit
Conventional	Dialog Semi. DA14580	3.4 mA	3 V	10.2 nJ/bit
Backscatter	MSP430 MCU Analog Osc. ADG918 RF Sw. **Total**	310 uA 305.4 uA 1.6 uA **623 uA**	2.5 V 2.5V 2.5V **2.5 V**	 **1.56 nJ/bit**

6.7 Chapter Conclusion

In this chapter, we present BLE Backscatter, an ultra-low-power approach to data uplink from a backscatter based sensor tag to existing smartphones or tablets equipped with a BLE chipset, without any modifications whatsoever to their hardware, firmware, or software. Building on our prior work with a test equipment based implementation [3], we present here a stand-alone, microcontroller based implementation of the BLE-Backscatter concept. This allows us to combine the power advantages of backscatter communication with the nearly ubiquitous availability of BLE chipsets in billions of existing smart phones, tablets, and PCs.

We demonstrate reception of the backscattered BLE advertising packets from the stand-alone BLE Backscatter tag with two unmodified BLE devices: an Apple iPad mini and a generic PC equipped with a Nordic Semiconductor nRF51882 BLE chipset. Each device successfully demodulates and accepts the advertising messages and passes them up the Bluetooth stack to the application layer. BLE Backscatter range of 13 meters is demonstrated using a +23 dBm EIRP fixed frequency carrier

source in the environment, with an unmodified Apple iPad mini. The BLE Backscatter tag consumes only 1.56 μJ/bit, over 6X lower power than the best commercially available BLE transmitters.

Future work includes integrating RF energy harvesting into the BLE-Backscatter tags to create a battery free BLE tag. Harvesting from a 2.4 GHz energy source such as a specially deployed CW source or ambient RF signals from Wi-Fi, BLE, or other 2.4 GHz transmissions would allow for a dual use of a single antenna on the tag. Such a tag would spend a majority of its time harvesting energy, switching periodically to the backscatter communication mode to generate BLE compatible packets to uplink sensor data. We will also conduct a more detailed investigation of the interference potential of the unwanted mixing products generated by the BLE-Backscatter tags, although we note that unwanted mixing products are a well known feature of existing backscatter devices; an image rejecting mixer approach could be considered to mitigate this issue by suppressing the unwanted sideband and its harmonics.

Finally, we expect that a future, integrated single-chip approach could substantially improve on our power result. For example, fixed-function logic to generate the outgoing bit stream would be lower power than the software based approach we used in this prototype. CMOS oscillators (such as those designed for conventional UHF RFID tags) generally have significantly lower power than the discrete bipolar oscillator that we used. Further, integration of a CMOS RF switch for backscatter modulation would reduce the amount of power needed to drive the switch compared with the board-level pads and wires in our prototype.

Chapter 7

Carrier options: modulated and unmodulated carriers

7.1 Introduction

Creating new ways to connect devices to the internet of things (IoT) requires new technologies but also attention to the patterns of technology adoption. Widespread use of a new technology will require some combination of significantly improved performance, lower cost, and ease of implementation compared to previously used solutions. Backscatter communication offers orders of magnitude lower power consumption compared to Bluetooth and Wi-Fi and yet for most wearable devices the preferred communication method is Bluetooth and Wi-Fi. These are widely deployed and established technologies and, critically, they have been adopted in most smart phones, laptops, routers, and smart home devices. The early lead and widespread adoption of these existing solutions make it more difficult for backscatter to break through as an alternative. Until recently it appeared that for backscatter to gain access to the valuable and growing areas of wearable devices backscatter readers would need to be incorporated into smart phones or be deployed on a large scale

in individual homes and offices. Even with the performance improvement for low power communication this implementation cost hurdle represented a big challenge for backscatter communication.

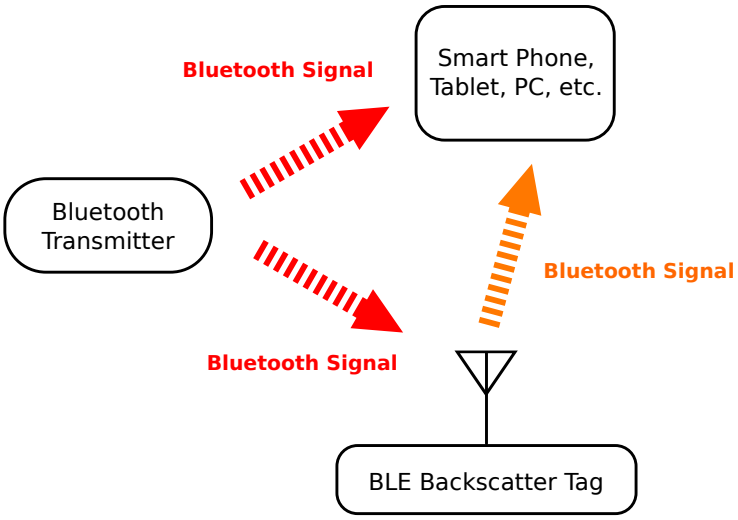


FIGURE 7.1: BLE backscatter using a BLE signal as a carrier source

Interestingly, it has recently been shown that backscatter devices can be created to communicate directly with existing wireless receivers. The technique of using conventional wireless receivers in backscatter systems was first demonstrated in [3] using BLE receivers and it has since been shown to also work with Wi-Fi and Zigbee receivers [103]. Achieving compatibility with the billions of existing conventional receivers solves part of the problem for allowing backscatter to be easily adopted. Because backscatter requires an external carrier source there are some additional complexities associated with a backscatter solution. Until smart phones have full duplex capabilities, the functions of carrier source and receiver will have to remain on two separate subsystems. The carrier source can come from any number of places including a dedicated transmitter, an access point, a smart home devices, or a smart phone. In [3, 46, 2] dedicated continuous wave (CW) transmitters were used as carrier sources. A modified BLE message was used by Iyer et. al to create a CW

signal for generating Wi-Fi and Zigbee backscatter packets [103]. This chapter will look into the requirements of the carrier source for generating BLE-Backscatter. We show that it is possible to create BLE-Backscatter with conventional data carrying BLE messages as illustrated in Fig. 7.1. A continuous wave carrier is not a requirement for producing BLE Backscatter messages; the 1 Mbps Gaussian shaped Binary Frequency Shift Keying (GFSK) modulation scheme used by BLE transmissions can also be used as a carrier signal. In this chapter we will discuss related works, provide an overview of BLE Backscatter, characterize the performance of a commercial BLE receiver and, finally, describe our results using BLE transmission as a carrier source for generating BLE Backscatter messages.

7.2 Related Work

Backscatter communication has been researched for decades, with the earliest examples using mechanical reflection of incident RF signals [32]. Since then many examples exist of using backscatter with custom backscatter readers. This includes work with conventional RFID protocols [104, 33, 35] and specialized protocols for communicating sensor data [105, 106]. Recent research has shown that conventional wireless receivers can also be used as backscatter readers with specially designed backscatter devices.

The most straightforward source for a carrier wave in these systems has been a CW signal either from an RFID reader or a custom built backscatter reader. There are some notable exceptions to using a CW source for backscatter communication, including for increasing the energy harvesting capabilities of a tag or for tag-to-tag communication. It has been shown that using signals with a high peak to average power ratio (PAPR) increases the energy harvesting efficiency of diode based harvesters as compared to a CW signal with the equivalent average power. These high PAPR signals go by the names of Power Optimized Waveforms (POW) [67], multi-

sine excitation [70], and chaotic waveforms [71]. To solve the forward link limitation of passive RFID tags, multifrequency signals were used for power transfer and as a carrier source for backscatter communication. Crucially, signals capable of providing an increase in harvesting efficiency were also shown to be adequate for data transfer. Another interesting approach used a data carrying signal, in this case a TV transmission, as a carrier signal for implementing backscatter communication [44]. With a custom two-antenna receiver, ambient backscatter communication was demonstrated at a range of greater than 80 feet and data rates of up to 1 Mbps with TV signals as the carrier source.

This chapter is focused on using commercially available BLE receivers with absolutely no modifications made to the receiver's hardware, firmware, or software. We investigate the requirements of the carrier source for creating backscatter signals that are compatible with unmodified BLE receivers.

7.3 BLE Receiver Requirements

Bluetooth Low Energy or Bluetooth Smart was designed as a low power communication standard targeting applications in wearable devices, wireless sensors, location awareness, healthcare, and security. With the adoption of Bluetooth 4.0 by major smart phone, tablet, and PC manufacturers it has rapidly become one of the dominant wireless connectivity solutions. BLE uses a 1 Mbps Gaussian shaped Binary Frequency Shift Keying (GFSK) modulation scheme. In each of the 40 BLE channels a positive frequency deviation of greater than 185 kHz above the channel's center frequency indicates a "1" bit and a negative frequency deviation of greater than 185 kHz below the channel's center frequency indicates a "0" bit.

As described in chapter 6, a BLE-Backscatter tag reflects a carrier signal to create a backscattered message containing frequency components at the desired frequency for a particular choice of BLE channel. When a CW signal is backscatter modulated

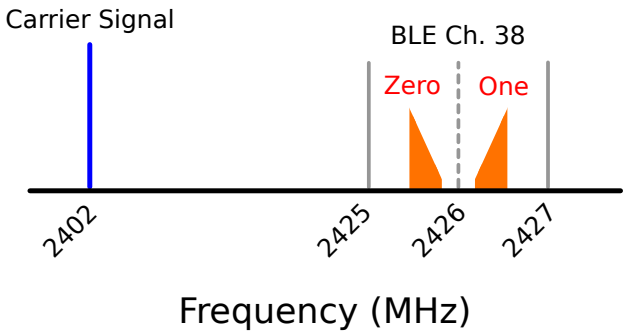


FIGURE 7.2: Example frequency plan, used in this chapter, for creating BLE compatible backscatter messages

with the modulated subcarrier, the resulting frequency components are:

$$M \cdot F_{carrier} \pm N \cdot (f_{sc} \pm \delta f_{sc}) \tag{7.1}$$

where $F_{carrier}$ is the frequency of the carrier, f_{sc} is the subcarrier frequency, and δf_{sc} is the subcarrier frequency deviation. As illustrated in Fig. 7.2, a possible frequency plan could have $F_{carrier}$ be a CW signal at 2402 MHz with a backscatter message designed for BLE channel 38. To accomplish this frequency plan, subcarrier frequencies of 23.75 and 24.25 MHz could be used. BLE channel center frequencies are spaced apart by 2 MHz allowing for a variety of subcarrier frequency options that would still be successfully received. In the following sections we describe experimental results showing the range of useful carrier and subcarrier signals for creating BLE Backscatter messages.

Frequency plans with harmonics

One way to increase the options for generating a frequency plan for BLE Backscatter devices is to take advantage of the harmonics generated in the backscatter process. An example frequency plan, from [3], uses a single CW frequency to produce backscatter messages in all three BLE advertising channels by using a combination of fundamental-mode and harmonic-mode backscatter signals. From Eq. 7.1, where

N is the subcarrier harmonic number, we choose N=1 to use the first harmonic of the subcarrier frequency. We can choose to map either the upper or lower sideband spectrum (USB/LSB) to a given BLE channel. Alternatively, as shown in Fig. 7.3, we can choose a center frequency F_{cw} at the midpoint between two BLE channels. In so doing, the upper sideband will communicate in the upper BLE channel with a normal spectrum (positive subcarrier deviation yields positive on-channel deviation), while the lower sideband will communicate in the lower BLE channel with an inverted spectrum (positive subcarrier deviation yields negative on-channel deviation). For BLE advertising channels 38 and 39, a center frequency $F_{cw} = 2453$ MHz with $f_{sc} = 27$ MHz serves Channel 38 from the LSB and Channel 39 from the USB. In this case the MBS transponder generates two subcarrier frequencies, $f_{sc,0}, f_{sc,1}$ where $|f_{sc,0} - f_{sc,1}| \geqslant 2$ x (185 kHz). In our initial proof of concept, we have chosen $f_{sc,0} = 26.7$ MHz and $f_{sc,1} = 27.3$ MHz for Channel 39 (USB). Note that the zero and one frequencies are flipped for Channel 38 (LSB). This is easily accommodated by simply inverting the outgoing data bits prior to transmission.

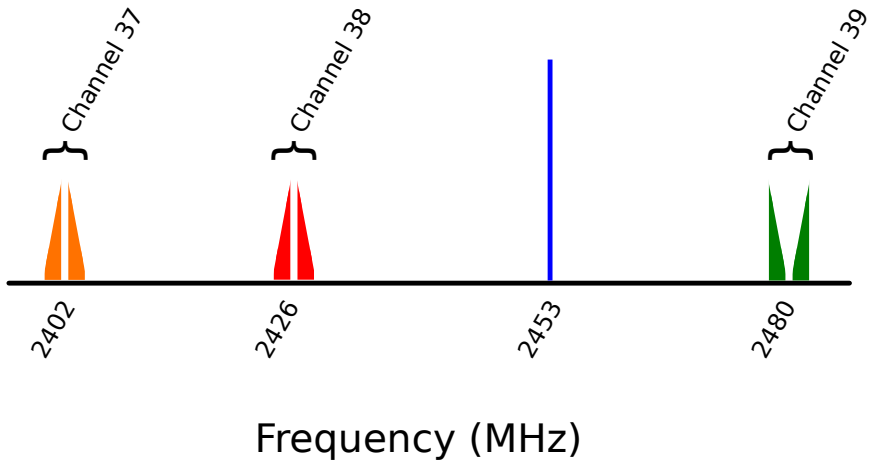


FIGURE 7.3: Frequency plan serving channels 38 and 39 using $N = 1$ and channel 37 with $N = 2$ from a fixed F_{cw}=2453 MHz

We leverage the harmonic mode (where $N > 1$) to serve other BLE channels from

the same F_{cw}. To serve Channel 37, which has a center frequency of 2402 MHz, we choose the lower side band, LSB, second harmonic with $N = 2$ and

$$f_{sc,0} = 25.5 + \delta f_{sc}/2 = 25.650 \text{ MHz}$$

$$f_{sc,1} = 25.5 - \delta f_{sc}/2 = 25.350 \text{ MHz}$$

as shown in Fig. 7.3. Note that in the harmonic mode, the subcarrier deviation must be reduced by a factor equal to the harmonic number N.

As was demonstrated in [3], advertisements were transmitted sequentially. The proof of concept transponder consists of a single BF1108 RF FET switch, Fig. 8.10(a) and a modulation source. For initial testing, the modulation source is an Agilent 33500B series arbitrary waveform generator (AWG). The AWG is used as a digital signal source so it would be straightforward to replace it with logic in an FPGA or ASIC. We have programmed the AWG to send three concatenated subcarrier modulated packets containing three distinct PDUs encoding device names {"Alice", "Bob", "Charlie"} on BLE advertising channels {37, 38, 39} respectively. A delay of 65μs was introduced between each of the packets. As previously described, the frequency plan shown in Fig. 7.3 allows a fixed CW frequency of 2453 MHz to serve all three advertising channels using the fundamental mode for channels 38 and 39, and the second harmonic mode for channel 37. A spectrogram of the concatenated sample vector is shown in Fig. 7.4. The first 232μs show the subcarrier frequencies required to generate an "Alice" packet using the second harmonic with N=2. Following a 65μs delay the subcarrier frequencies required to generate a "Bob" packet are displayed. Finally, after another 65μs delay the subcarrier frequencies for a "Charlie" packet are shown. We create all three BLE channels by backscattering a single incident CW carrier using a novel combination of fundamental-mode and harmonic-mode backscatter subcarrier modulation, with two of the band-pass channels generated by the fundamental mode and one of the band-pass channels generated by the second

harmonic mode. An unmodified Apple iPad is shown to correctly receive and display these packets at a range of over 9.4 m using its existing iOS Bluetooth stack with no changes whatsoever.

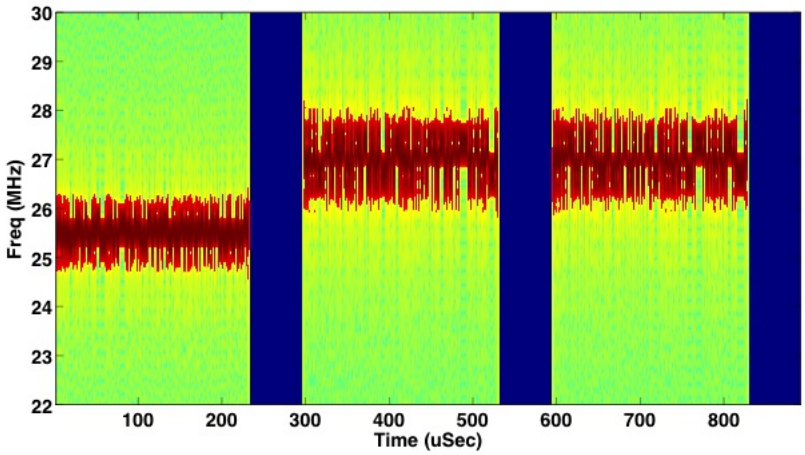


FIGURE 7.4: Spectrogram of three subcarrier modulated packets destined for BLE channels 37, 38, and 39 using the frequency plan described in Fig. 7.3.

7.4 Characterizing BLE receiver performance

To characterize the performance of a BLE receiver with our BLE-Backscatter signals, we focus on a cabled test setup to allow for controlled input powers to the BLE receiver. A block diagram of the cabled test setup is illustrated in Fig. 7.5. A carrier source is connected to the input of a directional coupler, and at the output of the coupler is our BLE-Backscatter tag. The BLE-Backscatter tag selectively reflects the carrier signal and a portion of the backscattered signal is fed into a Nordic Semiconductor nRF51822 evaluation board. Using the nRF Sniffer application together with Wireshark allows us to see the received packets and determine if they were decoded successfully without any bit errors. A photo of the evaluation board is shown in Fig. 7.6. The evaluation board has been modified to include an SMA input where there was originally a PCB trace antenna. This modification was made to facilitate

a cabled test setup.

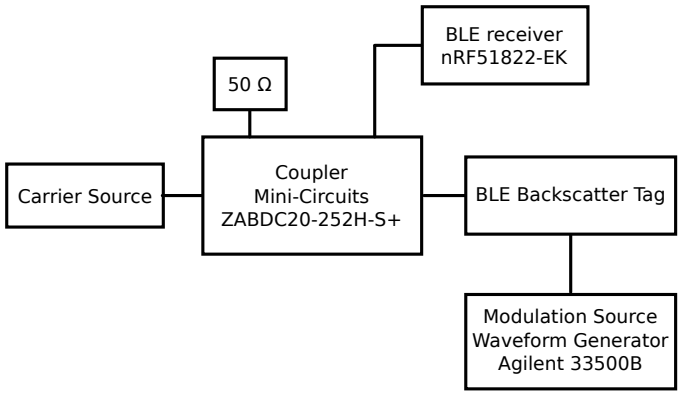


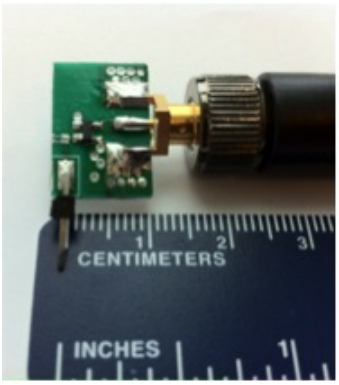
FIGURE 7.5: Cabled backscatter test setup

FIGURE 7.6: Modified nRF51822 evaluation board

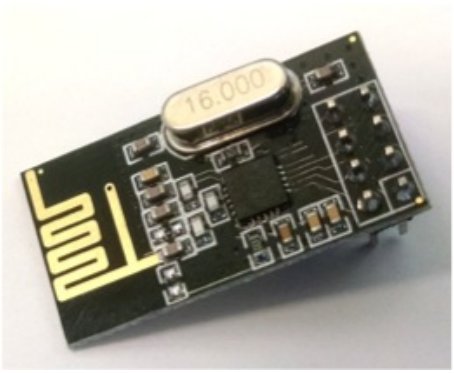
The BLE-Backscatter tag consists of a BF1108R modulating switch, Fig. 7.6, which is driven by an Agilent 33500B waveform generator. The waveform generator was used for the ease of implementing a variety of subcarrier frequency deviations, δf_{sc}, as compared to the BLE-Backscatter tag built with a custom hardware implementation discussed in Chapter 6.

7.4.1 CW Carrier Source

The example frequency plan from Fig. 7.2 uses a carrier signal that centers the backscattered signal in BLE channel 38. To determine the robustness of the BLE-Backscatter system, it is important to determine how far from the ideal value of 2402



(a)



(b)

FIGURE 7.7: (a) Photo of RF switch used for backscatter modulation (b) Photo of nRF24L01+ wireless transceiver module

MHz the CW signal can vary without severely impacting the BLE receiver's ability to correctly demodulate received packets. To answer this question, we used the cabled test setup with a CW carrier source coming from an Agilent N5181A signal generator. The CW source was varied from 2401.3 to 2402.9 MHz in 50 kHz steps with a backscattered message using subcarrier frequencies of 23.7 and 24.3 MHz. The same message was transmitted 10,000 times at each CW frequency and the percentage of error free messages was calculated. To properly center the BLE-Backscatter signal in BLE channel 38 (2426 MHz center frequency), the ideal value for the CW source is 2402 MHz. Fig. 7.8 shows a plot of the packet success rate with respect to the CW frequency.

The experimental measurements show that the CW carrier source may vary by up to 1.2 MHz without negatively impacting the BLE receiver's ability to decode BLE Backscatter messages. Both a positive and negative CW deviation of up to 500 kHz result in a received success rate of greater than 97%. The specific BLE receiver we tested has a slightly skewed response where a positive CW frequency deviation of up to 700 kHz still results in a packet success rate of greater than 97%. A significant amount of drift or uncertainty in the exact carrier frequency is thus expected to be

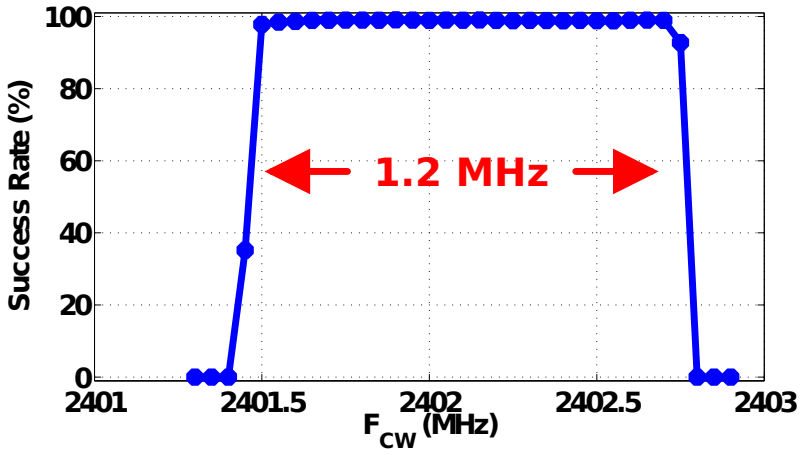


FIGURE 7.8: Packet success rate with CW source varying from the ideal value of 2402 MHz

acceptable for generating BLE-Backscatter messages.

7.4.2 BFSK Carrier Source

Based on the observation that the carrier signal can vary in such a way that the backscatter signal is significantly offset from the center frequency of the target channel, we next explore using a modulated carrier signal. The modulation used for the carrier signal is binary frequency shift keying (BFSK). For the measured data presented in this section, the BFSK carrier signal is centered at 2402 MHz and the frequency deviations are varied. The data rate for the BFSK carrier signal is 1 Mbps. A random sequence of ones and zeros was used as the data for the BFSK carrier signal, where a one corresponds to a positive frequency deviation and the zero corresponds to a negative frequency deviation. Every 1μs the subcarrier frequency is selected based on the random sequence of 0 and 1 bits.

Cabled measurements are performed with the test setup described in Fig. 7.5. The carrier source for these measurements is a BFSK signal generated with the test setup shown in Fig. 7.9. By using an Agilent 33500B series arbitrary waveform generator

we can define our signals in Matlab and quickly test the receiver's performance with a variety of BFSK carrier signals.

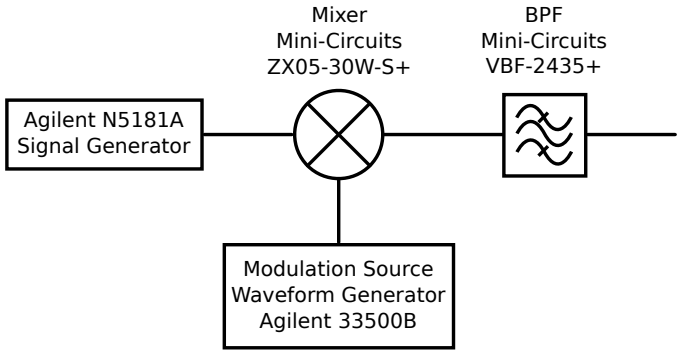


FIGURE 7.9: Test setup for generating BFSK carrier signal

Measurements are performed with BFSK deviations of ± 100 kHz, ± 150 kHz, ± 200 kHz, ± 250 kHz, and ± 300 kHz. In comparison to commercial transceiver the Texas Instruments CC2541 has frequency deviation options of 160 kHz and 320 kHz, [107], and the Nordic Semi nRF51822 has a frequency deviation of 250 kHz for BLE transmissions and 170 kHz for 1 Mbps Bluetooth transmissions [108]. The measured success rate of BLE-Backscatter packets is plotted vs. the received power for each of the different BFSK carrier signals in Fig 7.10. The received power is measured with an Agilent N9320B spectrum analyzer using the channel power function with a resolution bandwidth of 100 kHz as described in [45]. Once the channel power was measured at a relatively high input power level, ≈ -42 dBm, attenuators were added to vary the input power to the BLE receiver.

As power is spread out over a wider frequency range when the carrier modulation deviation increases, the RSSI value reported by the BLE receiver goes down. Spreading out the received signal in the frequency domain reduces the received power in the desired channel and makes packets more difficult to decode properly.

Interestingly, above a certain power level the packet success rate levels off for a given BFSK carrier signal. There appears to be a constant error rate associated

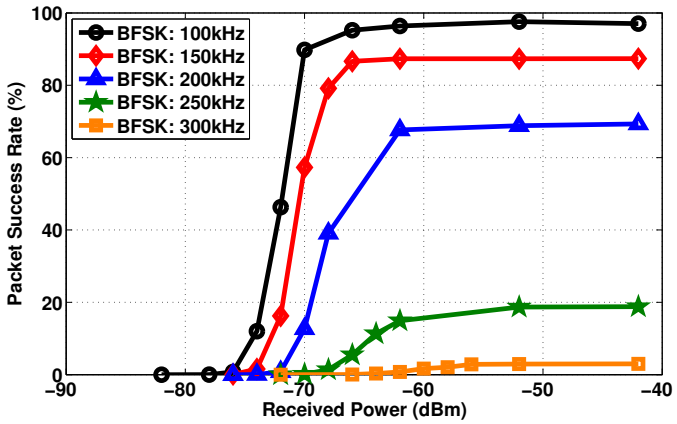


FIGURE 7.10: Packet success rate with BFSK carrier sources

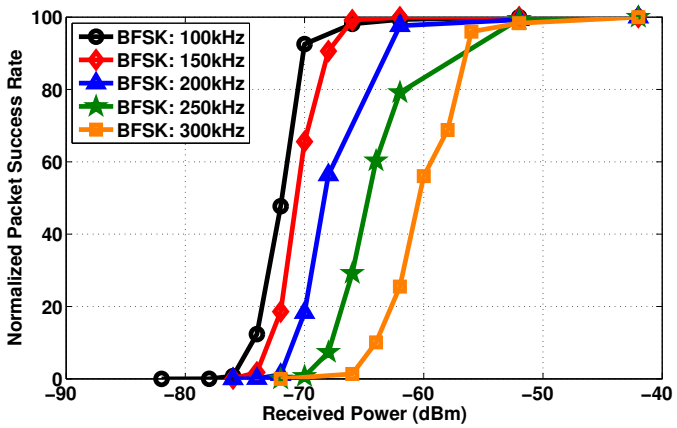


FIGURE 7.11: Normalized packet success rate with BFSK carrier sources, relative to the packet success rate with a received power of -42 dBm

with using a BFSK signal as the carrier. The wider the BFSK signal, the lower the success rate for a given received power. The input power at which the performance begins to degrade for each BFSK carrier also depends on the frequency spacing of the BFSK signal. As shown in Fig. 7.11 the decrease in performance, once the knee of each curve is reached, is relatively consistent. Relative to the maximum success rate for each BFSK carrier spacing, the performance drop associated with a decrease in received power is fairly constant.

7.5 Conventional BLE Messages as a Carrier

The Bluetooth 4.0 Low Energy spec has channels with a bandwidth of 2 MHz and a requirement for the subcarrier spacing of only +/- 185 kHz, leaving a significant range of frequencies that are assigned to either a "1" or "0" data bit. This opens the possibility for using a conventional BLE signal as the carrier while still having the backscatter message fall within the BLE spec. Unlike typical backscatter systems that use an unmodulated carrier, this is an example of modifying a communication signal containing data and inserting a new message with modulated backscatter. With this scheme a pair of BLE enabled devices, such as two smart phones, can act as both the carrier source and the receiver. For a single device to operate as both the carrier and receiver the BLE chipset would need to be able to operate in full duplex mode, simultaneously transmitting in one channel and receiving in another.

Using a BLE message as the carrier signal would allow for simultaneous transmission of a data carrying conventional BLE message and a BLE-Backscatter message. This could enable easy coordination of the carrier signal and receiving device since they would be communicating on a conventional wireless communication protocol. It may also be possible to leverage a device that is actively communicating to simultaneously serve as a carrier source. In this chapter we will exclusively use advertising packets as the conventional BLE transmission source but this technique would also work for transmission using BLE data channels since they use the same modulation scheme.

7.5.1 Packet Timing Considerations

One challenge when using a communication signal as the carrier, instead of a CW signal, is the brief transmission time of the communication signal. For the conventional BLE message to act as the carrier, the transmission must last for the full length of

the backscatter message. There must be full overlap of the conventional message and backscatter message for the backscatter device to constantly have a carrier source to selectively reflect.

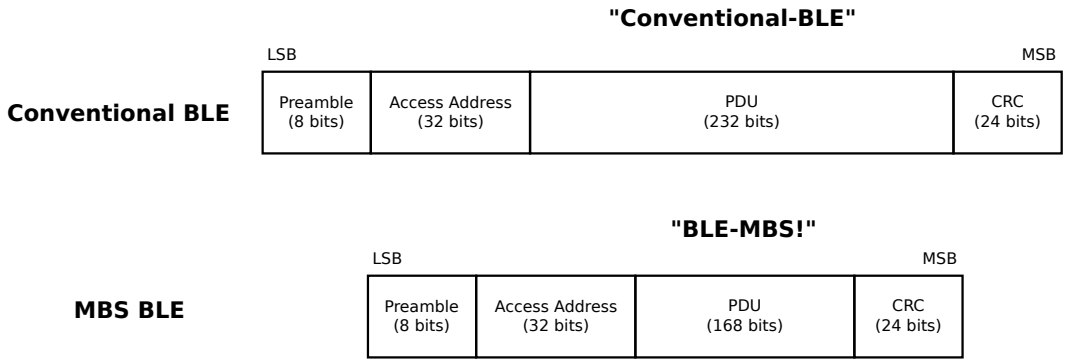


FIGURE 7.12: BLE packet format for conventional BLE message and BLE Backscatter message

In this work, we use advertising packets for both the conventional BLE transmission and backscattered BLE transmission. For a BLE packet there is a requirement for an 8 bit preamble, a 32 bit access address, a 24 bit CRC and a variable length payload data unit (PDU). To create a carrier BLE message that is longer than the backscatter window, we take advantage of the BLE advertising packet's variable length PDU. By using a PDU of 168 bits in the backscatter message and 232 bits in the conventional message, we are able to create a carrier signal that will last for the full duration of our backscatter message. As shown in Fig. 7.12 the BLE messages have been created to have device names "Conventional-BLE" and "BLE-MBS!" so they can be easily identified after being received. It is not important at what time during the conventional transmission backscattering begins, since there is no data coordination. The conventional transmission can contain any message. The use of the "Conventional-BLE" message as a device name is only to show that both the conventional message and backscattered message can be received successfully.

7.5.2 Frequency Plan

In addition to timing considerations, the other important factor is how a GFSK receiver interprets the backscattered signal. If a conventional BLE message is modulated such that the subcarrier frequency deviations are kept close to the minimum required in the BLE spec of +/- 185 kHz, a message from one channel can be backscattered to a new channel containing entirely new data. The original frequency deviation is still present in the backscattered signal, but it becomes a deviation contained entirely in the "0" or "1" frequency range as determined by the backscatter modulation.

The cartoon frequency plan shown in Fig. 7.13 uses a conventional BLE message created for channel 37 and illustrates in the frequency domain how that message can be backscattered to channel 38. This method will work with any BLE channels, so the use of channels 37 and 38 are referenced here as an example for demonstrating this idea. The message on channel 37 will contain device name "Conventional-BLE" and the backscattered message on channel 38 will contain device name "BLE-MSG!". The conventional signal is transmitting in channel 37 and it is switching between 2 FSK frequencies, at a 1 Mbps data rate. To meet the minimum frequency deviation spec of $\pm$ 185 kHz the binary frequencies would be 2401.815 MHz and 2402.185 MHz. Using this signal as a carrier is similar in concept to using a CW carrier that drifts quickly in time or has high phase noise. The exact carrier frequency is unknown but the range is specified, and that range is narrow enough to still be useful given the tolerance of the receiver to carrier offset.

The BLE transmission designed for channel 37 is then backscatter modulated with subcarrier frequencies of 24 MHz $\pm$ 500 kHz. The 500 kHz frequency deviation is able to shift either of the channel 37 frequencies to the "0" or "1" frequency range for channel 38. Since the carrier and backscattered message are both BLE packets,

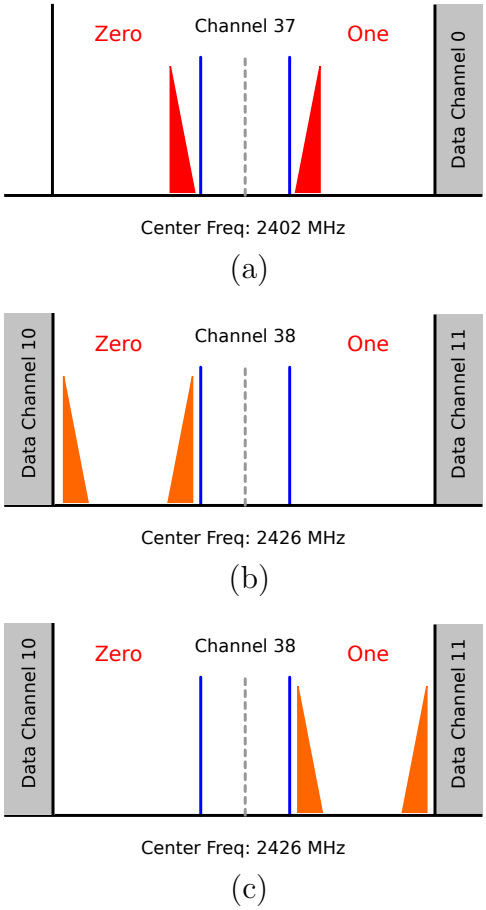


FIGURE 7.13: (a) Conventional BLE message (b) Scattered BLE message carrier to create a zero (c) Scattered BLE message carrier to create a one

the data rate of 1 Mbps is the same for both. That means there will be at most one carrier frequency deviation per bit in the backscattered signal. For example, over 1 us, which is the duration of 1 bit of the backscatter message, if the carrier message transitions from a "0" to a "1" and the backscatter data bit is a "1" the receiver will see first 2426.185 MHz and then 2426.685 MHz. Both 2426.185 MHz and 2426.685 MHz are received as a "1" data bit. Additionally, the conventional BLE signal has a continuous phase when transitioning between the two binary frequencies.

To verify the frequency plan, we use a cabled test setup with an nRF24L01+ acting as the conventional BLE source and a BF1108R switch controlled by an Agilent

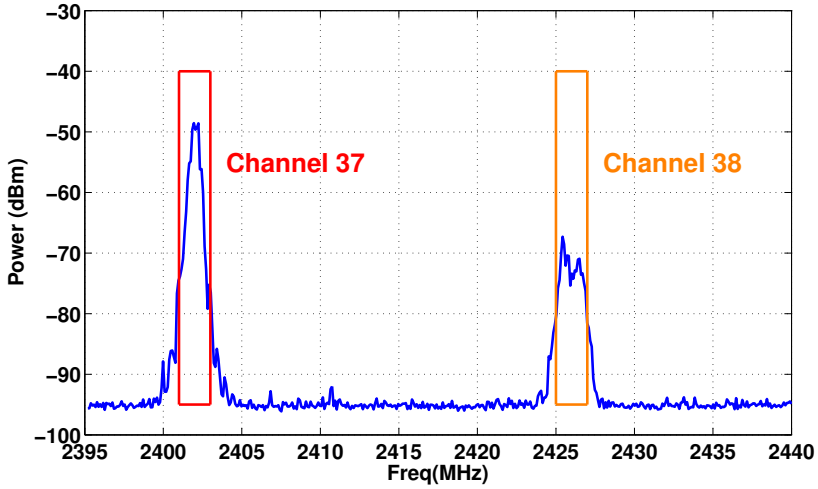


FIGURE 7.14: Cabled spectrum measurement showing a BLE message in advertising channel 37 and a Backscatter BLE message in advertising channel 38

33500B Waveform Generator as a backscatter device. The nRF24L01+ is set to transmit BLE advertising packets on channel 37 with a center frequency of 2402 MHz. Each packet is formatted to have a device name of "Conventional-BLE" and each message has a total length of 296 bits. The backscattered message is created with a subcarrier frequency of 24 MHz to operate in BLE channel 38, with a center frequency of 2426 MHz. Each BLE-Backscattered packet is 232 bits long with device name "BLE-MBS!".

Fig. 7.14 shows that, as expected, there are signals in both channel 37 and 38. As expected the backscattered signal in channel 38 has a wider frequency spread than the conventional BLE message in channel 37. After validating the frequency plan, the next step involves testing the BLE-Backscatter system in an over the air test.

7.5.3 OTA Testing

The test setup for our over the air (OTA) testing involved a carrier source separated from the BLE-Backscatter tag by a distance, D1, and the BLE-Backscatter tag separated from a BLE receiver by a distance, D2, as shown in Fig. 7.15. The carrier

source used in this test was a Nordic Semiconductor nRF24L01+ wireless transceiver, Fig. 8.10(b). The nRF24L01+ wireless transceiver module was controlled using an Arduino Nano. As was the case in Section 7.4 the backscatter device consists of a BF1108R switch controlled by an Agilent 33500B Waveform Generator. The receiver is also the same as the one used in Section 7.4 but now a dipole antenna has been used instead of a cabled connection.

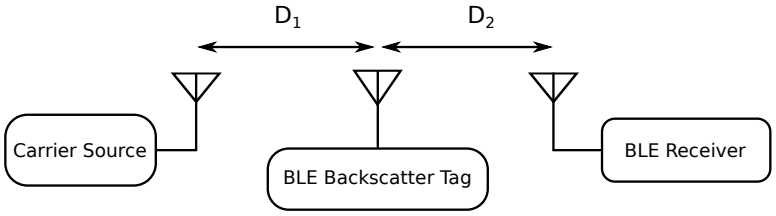


FIGURE 7.15: OTA test setup diagram

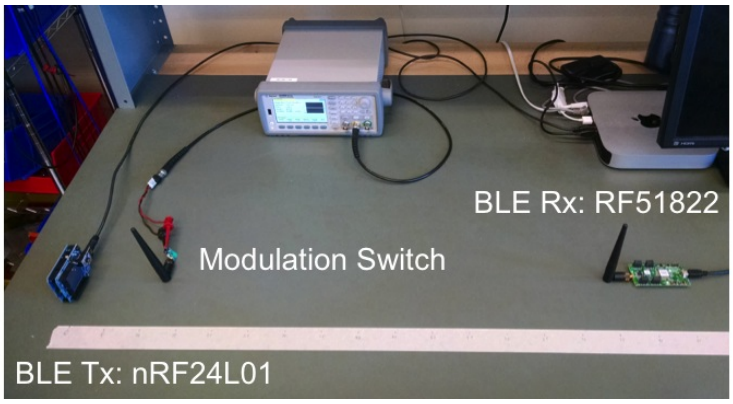


FIGURE 7.16: Photo of OTA test setup

By using the nRF sniffer together with Wireshark we can view the received packets on channel 38 produced by our BLE-Backscatter tag. For each successfully received packet the RSSI is also reported. For each receiver measurement location, D2 from 10 cm to 115 cm in 5 cm steps, recordings were measured for a 1 minute interval. Even at the same measurement location the reported RSSI varied by as much as 10 dB. Fig. 7.17 shows the maximum, average, and minimum RSSI for successfully received packets in the 1 minute recording interval. At 90 cm the maximum, average,

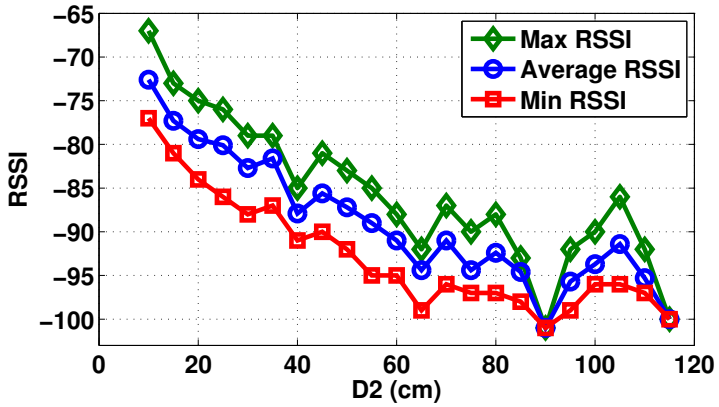


FIGURE 7.17: Reported RSSI (arbitrary dB units) with the distance between the BLE transmitter and BLE Backscatter tag separated by 10 cm

and minimum RSSI have identical values because each successfully received packet is at the lower limit of what can be received by the nRF24L01+ receiver.

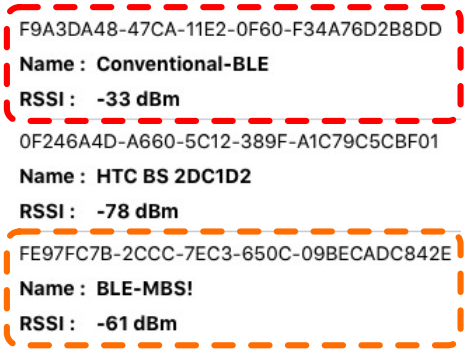


FIGURE 7.18: Cropped screen shot of Apple iPad Mini running a BLE scanner app showing a successfully received and decoded conventional BLE message and BLE-Backscatter message

With an unmodified Apple iPad mini running a BLE scanner app, we were able to see both the carrier signal, "Conventional-BLE", and backscattered signal, "BLE-MBS!". In our lab area there are many other BLE advertising packets that were also picked up by the iPad mini. We have cropped out many of the other devices to more clearly show the packets of interests for this experiment. As expected the reported RSSI for the conventional transmission was significantly higher, approximately 28 dB

higher, than the backscattered transmission. The iPad mini is able to successfully decode the weaker backscatter signal because of the 24 MHz of frequency separation between BLE advertising channels 37 and 38. The interference performance of the BLE receiver is covered in detail in Chapter 8.

7.6 Chapter Conclusion

Recent work on backscatter communication has continued to push the low power communication technique as a potential solution for connecting the internet of things. This chapter explores the requirements of the carrier source for creating BLE-Backscatter messages. We demonstrate that conventional BLE messages can be used as a carrier source for BLE-Backscatter messages. The only required information about the conventional BLE message is the operating channel frequency. Advance knowledge of the contents of the conventional BLE packet are not required to receive the backscattered message with an unmodified BLE receiver.

Chapter 8

Communication Distance Achievable for BLE-Backscatter

Limiting factors for operating BLE-Backscatter devices are explored for monstatic and bistatic setups. A characterization of a commercially available BLE receiver is conducted to understand the performance limits of a BLE-Backscatter system. The characterization focuses on the receiver sensitivity and interference rejection performance of the receiver, both of which influence the achievable communication distance. Interference mitigation techniques are explored and implemented for monostatic and bistatic systems. In the monostatic setup a range of 3 m is achieved by implementing a carrier suppression circuit. A range of greater than 30 m is demonstrated for the bistatic setup where the receiver and BLE Backscatter devices are in a physically paired configuration.

8.1 BLE Receiver Sensitivity

The receiver sensitivity listed by Bluetooth transceiver chip manufacturers is the receiver sensitivity without any interference sources in the environment. The receiver

sensitivity depends on signal to noise ratio (SNR) at the receiver resulting from thermal noise and noise added by the receiver itself. The thermal noise power can be calculated easily if the receive bandwidth is known. The equation for the received noise power is:

$$P_n = kTB \tag{8.1}$$

where k is the Boltzmann constant ($1.38064852 \times 10^{-23} J/K$), T is the temperature in Kelvin, and B is the system bandwidth in hertz. Assuming the receiver is at room temperature, 293 K, with a typical BLE receiver bandwidth of 2 MHz the thermal noise power is $P_n = -110.9$ dBm, from Eq. 8.1. This is the input noise level to the receiver, but various components in the receiver decrease the signal to noise ratio as the signal propagates through the receiver.

In a typical BLE receiver, the first component in the receiver chain is a low noise amplifier (LNA), followed by a mixer and an IF stage. The noise figure, F, of the receiver is defined as:

$$F = \frac{S_i/N_i}{S_o/N_o} \tag{8.2}$$

where S_i/N_i is the input signal to noise ratio and S_o/N_o is the output signal to noise ratio. Typical low cost CMOS receivers in the 2.4 GHz band have a noise figure on the order of 5 dB. Further, to receive a BFSK signal with a low probability of a bit error (BER $\leqslant$ 0.1%), an SNR of at least 7 dB is required. This puts our final receiver input power requirement at $P_r >= P_n + F + BFSK_{SNR}$ or -98.9 dBm. The manufacturer's specified receiver sensitivities of a number of BLE receivers are listed in Table 8.1 below. With receiver sensitivities ranging from -92 dBm to -95 dBm these receivers are close to the minimum we expect from our quick thermal noise evaluation.

Table 8.1: BLE receiver sensitivity requirements and typical performance of commercially available Bluetooth ICs

Manufacturer	**Device Name**	**Receiver Sensitivity (dBm)**
Nordic Semiconductor	nRF51822 [108]	-93
Texas Instruments	CC2540F128 [107]	-93
Dialog Semiconductor	DA14580 [109]	-93
Silicon Lab	Bluegiga BLE112 [110]	-92
NXP	QN902 [111]	-95

To test the receiver sensitivity of a conventional transceiver in Bluetooth low energy mode, cabled experiments are performed with a Nordic Semiconductor nRF24L01+ transceiver IC acting as a repeatable source of BLE transmissions. The transmitter is configured to transmit a known BLE advertising packet with device name "Alice" in advertising channel 38. The cabled measurement setup is shown in Fig. 8.1. The nRF24L01+ prototype board has a PCB trace antenna and therefore can't be directly connected to our cabled test setup. To acquire a known power level from the transmitter we place the transmitter unit inside a metal shielding container along with a 2.4 GHz dipole antenna. With a fixed antenna spacing inside the container we measure the received power at the output of the 2.4 GHz dipole and feed the received signal from the dipole to the BLE receiver being tested, through a known attenuator and power splitter, keeping track of the input power to the receiver. By varying the attenuator we are able to control the input power to the receiver. The cabled test setup described in Fig. 8.1 shows a signal generator also connected to the power splitter feeding the receiver. For the receiver sensitivity measurements the signal generator has no output. The signal generator is used for later experiments to characterize the receiver performance in the presence of an interference source. The BLE receiver used in this experiment is a Nordic Semiconductor nRF51822 Bluetooth transceiver, Fig. 7.6. Each received packet is analyzed to determine if there are any errors in the decoded packet and to set a packet error rate (PER) for various

receiver input powers..

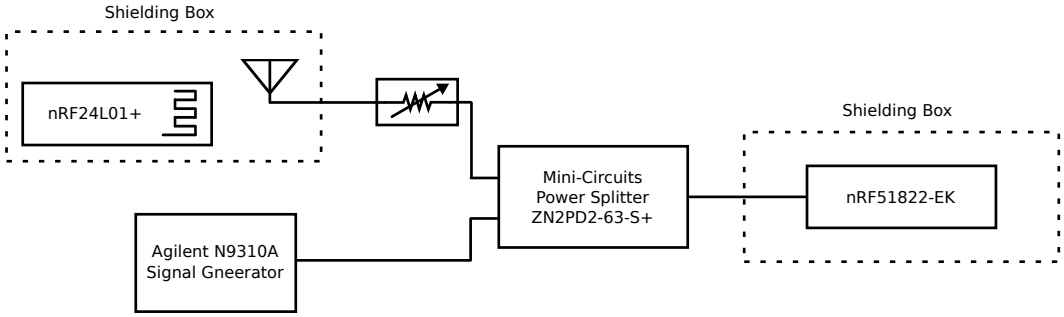


FIGURE 8.1: Cabled test setup for characterizing BLE receiver

Fig. 8.2 shows a plot of the PER as a function of input power to the nRF51822 Bluetooth transceiver. The receiver sensitivity is defined as the input power for which the bit error rate (BER) $\leqslant 0.1\%$. For our 232 bit packets, assuming independent errors, this corresponds to a PER of 20.7% ($1 - .999^{232}$). The minimum receiver sensitivity for devices meeting the Bluetooth specification is -70 dBm and the typical receiver sensitivity for the Nordic Semiconductor nRF51822 is specified by the manufacturer as -93 dBm. The measured receiver sensitivity of the nRF51822 evaluation board is -83 dBm. The reduced sensitivity compared to the typical value from the manufacturer's specification comes from two main sources; mismatch losses introduced by replacing the PCB antenna of the evaluation board with a coaxial connector and the losses in the discrete matching network on the evaluation board. As shown in Fig. 8.2, the measured receiver sensitivity, the minimum input power for which the PER $\leqslant 20.7\%$ is significantly below the -70 dBm minimum set by the Bluetooth SIG. The measured PER using the nRF51822 receiver is nearly zero when the input power is greater than -76 dBm. The PER increases as the input power decreases from -76 dBm to -96 dBm leveling off at a 100% PER with input powers at or below -96 dBm.

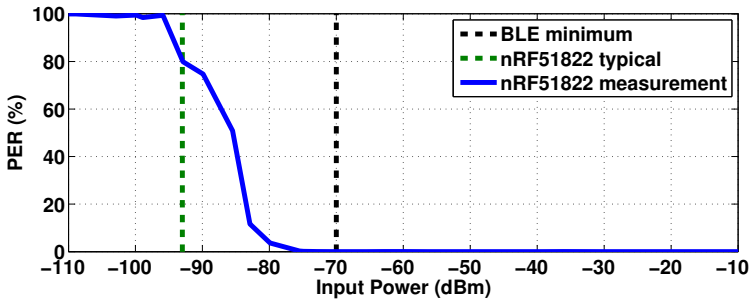


FIGURE 8.2: Measured PER vs. received BLE power for a Nordic Semiconductor nRF58122 evaluation board

8.2 Self-jamming due to the carrier

In conventional, active radios Bluetooth receivers are limited by the receiver sensitivity and interference performance. Nearby transmitters may be transmitting at the same or nearby frequency to the receiver's operating frequency. Conventional Bluetooth devices have several ways to deal with interfering signals. There are certain performance requirements BLE receivers must meet even in the presence of high power interference sources at nearby frequencies. Conventional Bluetooth devices also use frequency hopping schemes to prevent one device from constantly jamming another by operating in the same or adjacent Bluetooth channels. Additionally, conventional Bluetooth transmissions can repeat messages in order to avoid overlapping transmissions in time. In a backscatter scenario, there is a constant source of interference, or self-jamming, coming from the external carrier signal source. The carrier signal can be co-located with the receiver, in a monostatic setup, or exist in a separate device, in a bistatic setup. In both scenarios the receiver has to contend with the high power carrier source desensitizing the receiver to the desired BLE-Backscatter transmission. Understanding the performance of a commercial Bluetooth receiver with a single tone interference source will help in characterizing the performance of a BLE-Backscatter system as well as defining the crucial parameters required for

successful deployment of future BLE-Backscatter devices.

8.2.1 Blocker Specifications

The Bluetooth SIG defines a minimum interference rejection performance for certified Bluetooth receivers. Table 8.2 summarizes the specifications outlined in [45] and the manufacturer's specified performance for three commercially available BLE transceivers, including the nRF51822 transceiver used in our measurements. These interference performance values are defined for Bluetooth interference sources where the interference signal is modulated according to the BLE specifications. For example, according to the Bluetooth requirements, if an interference source is offset by 4 MHz from the desired signal's channel frequency, the receiver should be able to decode the desired signal with a signal to interference ratio (SIR) of -27 dB. The performance listed for the nRF51822 transceiver only has to meet this minimum to be certified but for a 4 MHz offset the manufacture's specified SIR is -51 dB.

Table 8.2: Interference performance requirements for BLE receivers and typical performance of commercially available Bluetooth ICs

	BLE Spec	**nRF51822**	**QN902**	**DA14580**
Co-Channel , $C/I_{co-channel}$	21 dB	10 dB	7 dB	6 dB
Adjacent (1 MHz), C/I_{1MHz}	15 dB	1 dB	-3 dB	-1 dB
Adjacent (2 MHz), C/I_{2MHz}	-17 dB	-25 dB	-30 dB	-40 dB
Adjacent ($\geqslant$ 3 MHz), $C/I_{\geqslant 3MHz}$	-27 dB	-51 dB	-35 dB	-40 dB

Experimental measurements of the receiver's interference rejection performance were conducted with the cabled test set up in Fig. 8.1. As with the receiver sensitivity measurements, the source of our desired BLE packets is from a Nordic Seminconductor nRF24LO01+ transceiver. The interference source is a CW signal coming from an Agilent N9310A signal generator. The BLE and CW signals are combined using a Mini-Circuits ZN2PD2-63-S+ power splitter. The combined signals are then cabled

directly to the nRF51822 receiver. Both the Bluetooth transmitter and receiver are placed in shielding boxes to minimize the influence of wireless transmissions from nearby Wi-Fi and Bluetooth devices in the lab. The input power from the BLE transmitter to the receiver is adjusted by changing the attenuator shown in Fig. 8.1.

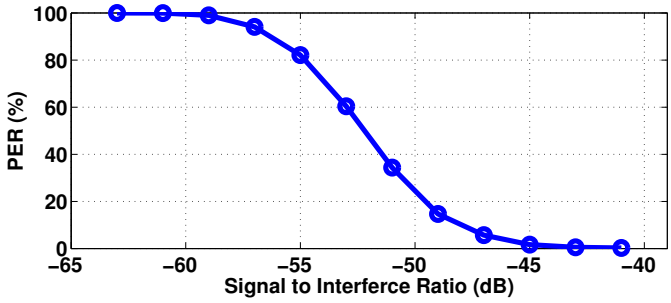


FIGURE 8.3: Sample measurement showing PER as a function of SIR with a BLE signal at 2426 MHz and a CW interferer at 2412 MHz

All measurements in this section were performed with a BLE input power of approximately -74 dBm. All BLE transmissions have device name "Alice" and are broadcast on advertising channel 38. Interference measurements are then performed with the signal generator set to a variety of frequencies and input powers to determine the SIR with an acceptable packet error rate (PER $\leqslant$ 20.7%) at a number of interference offset frequencies. A sample result is shown in Fig. 8.3. The interference source is set at a 14 MHz offset frequency from the desired BLE transmission and the PER is measured with a number of interference input powers ranging from -33 dBm to -11 dBm. When the SIR is at or above -42 dB the received packet error rate is $\approx$ 0% for 10,000 total receiver packets. The PER increases between SIR values of -43 dB to -62 dB until the PER reaches 100%. With an interference source at 2412 MHz the Nordic Semiconductor nRF51822 transceiver is able to receive BLE packets with a BER $\leqslant$ 0.1% at 2426 MHz when the power of the CW interference source is 49 dB higher than the desired BLE signal.

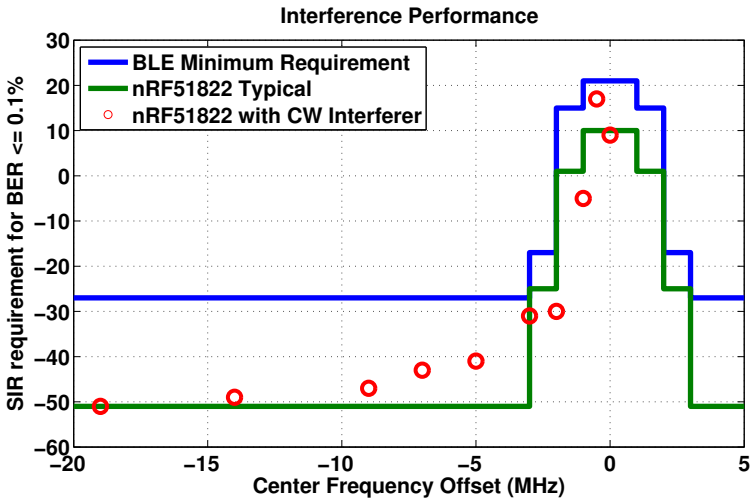


FIGURE 8.4: Measured interference performance with a CW interferer using an nRF51822 evaluation board as a BLE receiver

The results of the interference measurements are summarized in Fig. 8.4. The BLE minimum requirements are plotted in blue and the typical values provided by the manufacturer from the nRF51822 transceiver are plotted in green. The red data points indicate the measured minimum SIR for a BER $\leqslant 0.1\%$. The measured interference performance shows that, as expected, a greater frequency difference between the carrier source and desired BLE frequency results in better rejection of the carrier by the receiver. From these measurements there appears to be diminishing returns beyond a 9 MHz carrier offset frequency. For a BLE-Backscatter system the subcarrier frequencies generated by the tag determine the offset frequency from the self-jamming carrier source and BLE-Backscatter signal. Increasing the subcarrier frequency will reduce the effect of the self-jamming carrier source at the cost of a greater energy expenditure at the BLE-Backscatter tag as described in section 6.6.3, Energy Savings of BLE-Backscatter vs Conventional BLE. It is also important to note that the minimum requirement given by the Bluetooth specification does not call for improved interference rejection beyond a 3 MHz offset from the receiver's center frequency. Individual manufacturers may exceed the performance specifications

outlined by the Bluetooth specification but there is no guarantee that a particular device will have an interference rejection performance beyond the Bluetooth minimum plotted in Fig. 8.4

8.3 Received Backscatter Power

To understand the influence of the receiver sensitivity and interference rejection performance on a BLE-Backscatter system we have to understand the expected received signal power of both the BLE-Backscatter signal and carrier signal. From this analysis we will see how the performance of the system depends on the deployment scenario.

Bistatic Configuration

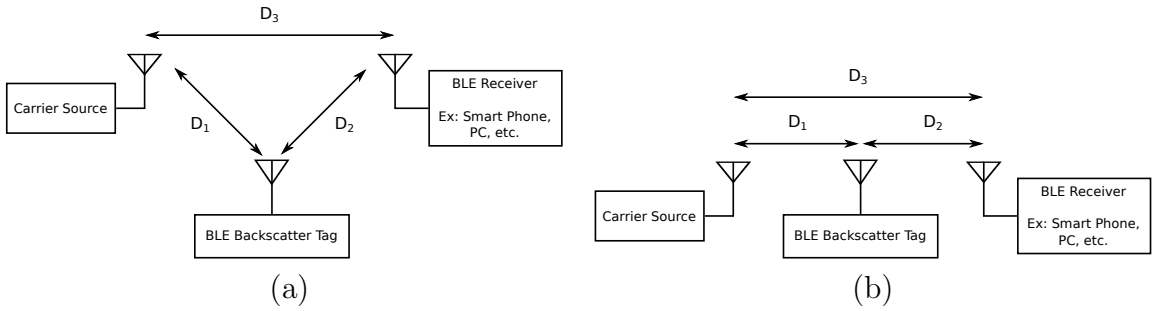


FIGURE 8.5: (a) General bistatic backscatter block diagram (b) Straight line bistatic backscatter block diagram

A link budget based on the approach of [100] was calculated to estimate the operating range of a BLE-Backscatter tag. In a scenario with a physically separated carrier source and BLE receiver the BLE-Backscatter system is similar to a bistatic radar setup. The received power at the BLE receiver is calculated as the product of two parts. Referring to the geometry of Fig. 8.5a., the backscattered power available from the tag is

$$P_{tag} = \frac{P_t G_t \Delta\sigma}{4\pi D_1^2} \tag{8.3}$$

where D_1 is the distance from the carrier source to the tag, P_t and G_t are the carrier source output power and gain of the transmitting antenna respectively, and $\Delta\sigma$ is the differential radar cross section (RCS) [101, 102, 83] given by

$$\Delta\sigma = \frac{\lambda^2}{4\pi} G_N^2 \left|\Gamma_1^* - \Gamma_2^*\right|^2 \tag{8.4}$$

where G_N is the antenna gain of the node (tag) and Γ^* is the conjugate match reflection coefficient

$$\Gamma^* = \frac{Z_a^* - Z_L}{Z_a + Z_L} \tag{8.5}$$

for a resonant antenna impedance Z_a and the complex load impedance Z_L. The power received at the BLE receiver (e.g. a smartphone) is

$$P_{R,BLE} = \frac{P_{tag} G_r \lambda^2}{(4\pi)^2 D_2^2} \tag{8.6}$$

where G_r is the gain of the receiver's antenna and D_2 is the distance from the tag to the BLE receiver.

Combining Equations 8.6 and 8.4 gives the backscattered power at the BLE receiver, assuming that antenna gains and transponder RCS are in the preferred orientation

$$P_{R,BLE} = \frac{P_t G_t \Delta\sigma G_r \lambda^2}{(4\pi)^3 D_1^2 D_2^2} \tag{8.7}$$

In addition to the backscattered signal at the receiver, there is a self-jamming signal coming from the carrier source. The backscattered signal is offset in frequency from the carrier signal but to understand the influence on the receiver we need to determine the SIR where the desired signal is the BLE-Bluetooth signal and the interference is coming from the carrier. Using the geometry of Fig. 8.5(a). the carrier signal power at the receiver is

$$P_{R,Carrier} = \frac{P_t G_r \lambda^2}{(4\pi)^2 D_3^2} \tag{8.8}$$

where D_3 is the distance from the carrier source to the BLE receiver. The SIR is then

$$SIR = \frac{P_{R,BLE}}{P_{R,Carrier}} \tag{8.9}$$

or

$$SIR = \frac{P_t G_t \Delta\sigma G_r \lambda^2 (4\pi)^2 D_3^2}{P_t G_t G_r \lambda^2 (4\pi)^3 D_1^2 D_2^2} \tag{8.10}$$

which reduces to

$$SIR = \frac{\Delta\sigma D_3^2}{(4\pi) D_1^2 D_2^2} \tag{8.11}$$

Interestingly, Eq. 8.11 suggests that the SIR is independent of the transmit power and is determined largely from the geometry of the backscatter setup.

To see the impact of the blocker performance on the range in our bistatic setup we compare the theoretical received power from the backscatter device with the theoretical received power from the carrier source as described in Eqs. 8.8 and 8.7. We use measured data from the BLE-Backscatter tag described in Chapter 6 to model the backscatter power.

The carrier source and tag antennas are dipole whip antennas with 2.1 dBi gain. We have assumed that the gain of the BLE antenna in the Apple iPad mini or smart phone, acting as a BLE receiver, is approximately 0 dBi. Values for Z_{L1} and Z_{L2} were measured over the 2400 MHz to 2483 MHz band with modulating RF switch control voltages of 0.4 and 0.5 V, representing either side of the measured logic threshold of the ADG918 switch. Measurements shown in Fig. 8.6 were performed with an Agilent N5222A PNA network analyzer at the SMA port of a stand-alone

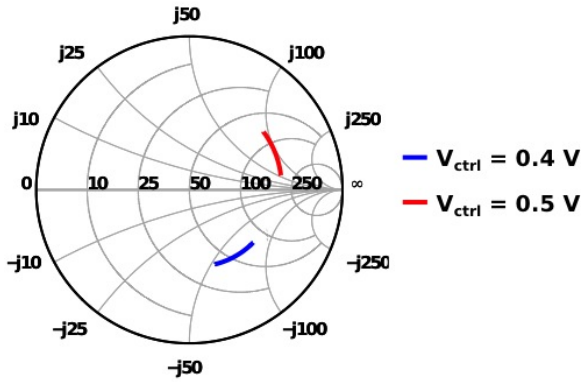


FIGURE 8.6: Measured S_{11} of ADG918 over 2400-2480 MHz, V_{ctrl} = 0.4 V and 0.5 V.

test board. The values of Z_{L1} and Z_{L2} at 2414 MHz were used in our link budget calculation since that is the mid point between BLE advertising channels 37 and 38.

Table 8.3: Parameters for bistatic link budget calculation

λ	0.124 meters
P_t	+33.9 dBm, +23.9 dBm, +13.9 dBm
G_t	2.1 dBi
G_N	2.1 dBi
G_r	0 dBi (estimated)
Z_a	50 + j 0 Ω
Z_{L1}	76 - j 74 Ω
Z_{L2}	78 + j 93 Ω

Using the straight line bistatic setup shown in Fig. 8.5b. we have calculated the expected received power of the BLE-Backscatter signal and carrier signal. In Fig. 8.7 the theoretical received powers for the carrier signal are plotted as solid lines and BLE-Backscatter powers as dashed lines. The three sets of colored lines are for carrier transmit powers of +36 dBm, +26 dBm, and +16 dBm EIRP. Additionally, Fig. 8.7 shows a solid black line at 0 dBm and a dashed black line at -93 dBm indicating the manufacturer's specified maximum received signal strength and receiver sensitivity respectively, for the Nordic Semiconductor nRF58122 transceiver. A total carrier

source to BLE receiver distance, $D_1 + D_2$, of 13 m is used because that is the distance for which backscattered powers were collected in Fig. 6.15 of Chapter 6. The expected carrier source power at the BLE receiver does not depend on the BLE-Backscatter tag location and as a result, the expected carrier source power depends on the transmit power but not on distance D_1. The expected BLE-Backscatter power depends on both the transmit power of the carrier source, P_{Tx}, and the distance D_1. For a given transmit power the received BLE-Backscatter power forms a bathtub curve where the power is maximized when the BLE-Backscatter tag is close to either the carrier source ($D_1 = 0$ m) or receiver ($D_1 = 13$ m).

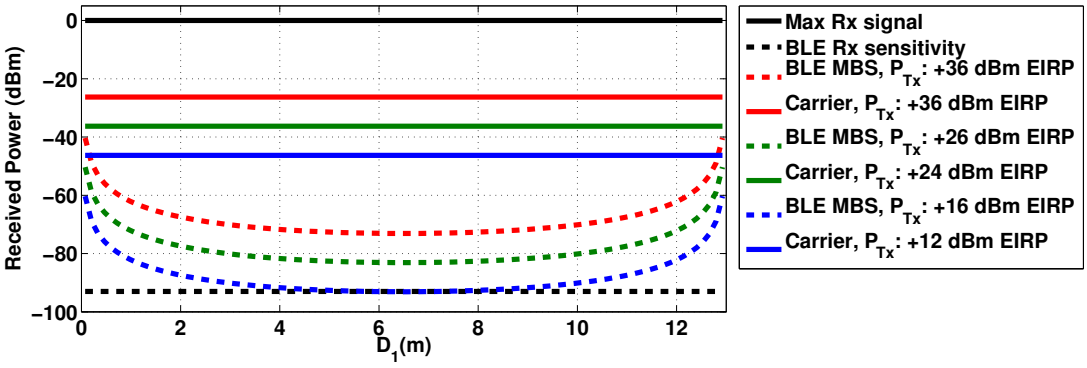


FIGURE 8.7: Receiver power levels for straight line bistatic setup, $D_1 + D_2 = 13$ m

As we can see from Fig. 8.8 the SIR also forms a bathtub curve, where the desired signal is the BLE-Backscatter signal and the interference is from the self-jamming carrier source. The SIR is maximized when the BLE-Backscatter tag is close to either the carrier source or receiver and the SIR is at a minimum when the BLE-Backscatter tag is directly between the carrier source and receiver. Since both the BLE-Backscatter signal power and carrier source signal power depend on the transmit power of the carrier source the SIR is the same for all transmit powers and depends only on the distance D_1. Fig. 8.8 also shows two dotted lines representing the SIR required for a PER $\leqslant 20.7\%$ with a self-jamming carrier signal 9 MHz away

from the BLE-Backscatter frequency.

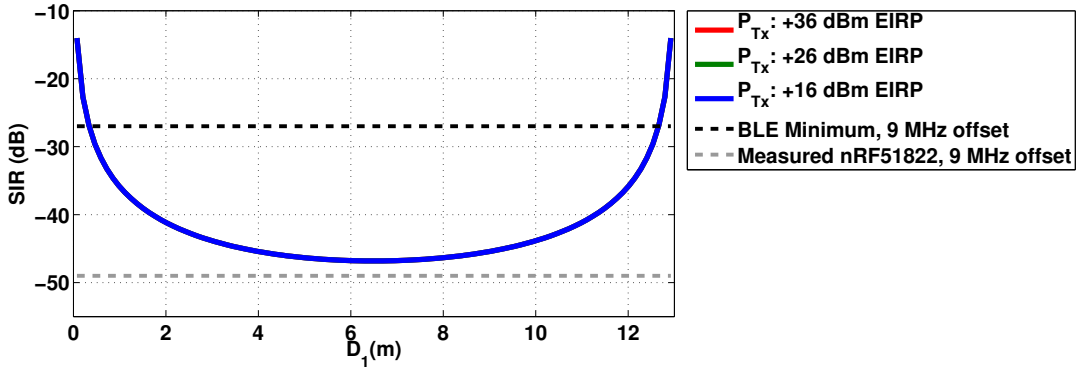
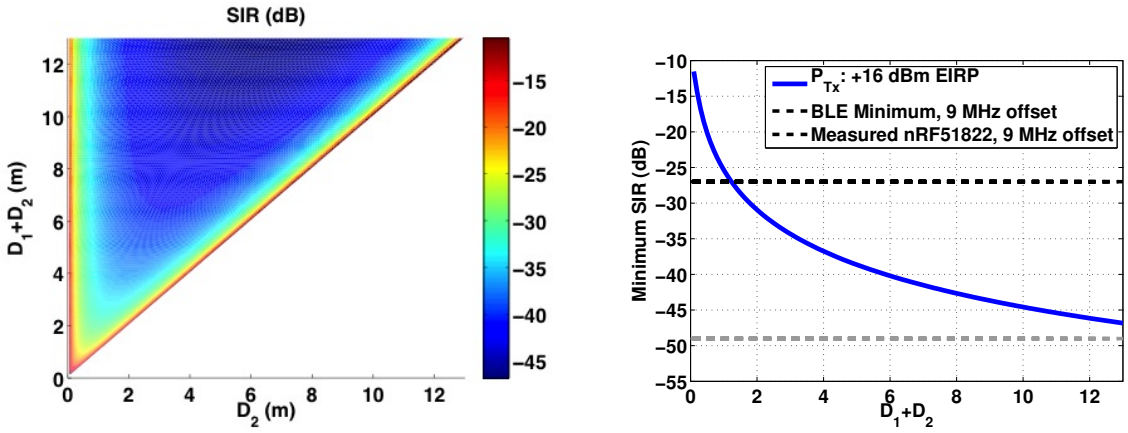


FIGURE 8.8: SIR for straight line bistatic setup, $D_1 + D_2 = 13$ m

These theoretical SIR curves help explain why we were able to successfully receive BLE-Backscatter packets in the OTA tests summarized in Fig. 6.15 of Chapter 6. If the BLE receiver in the Apple iPad mini used in those experiments has a similar performance to the Nordic Semiconductor nRF51822 transceiver, then with a 13 m separation between the carrier source and receiver we were operating just inside the SIR margin for successful reception of BLE-Backscatter packets at tag locations directly between the carrier source and receiver. By allowing ourselves to slightly reposition the Apple iPad mini we avoided multipath nulls and locations that would have similarly minimized the received SIR.

To see how the SIR changes as a function of carrier to receiver separation distance, $D_1 + D_2$, Fig. 8.9 shows a 2D illustration of SIR varying with changes in $D_1 + D_2$ and D_2, the tag to receiver distance. As in Fig. 8.8 the SIR is minimized when $D_2 = \frac{D_1+D_2}{2}$. Fig. 8.9b is a cut from Fig. 8.9(a) showing only the minimum value of SIR as a function of $D_1 + D_2$. This shows the SIR performance required of a receiver for a successfully deployed bistatic setup given a particular carrier to receiver separation. To ensure meeting only the BLE minimum SIR specification the carrier source must be quite close to the BLE receiver. As the gray dotted line in



(a) (b)

FIGURE 8.9: (a) SIR for straight-line bistatic setup (b) Minimum SIR for straight-line bistatic setup

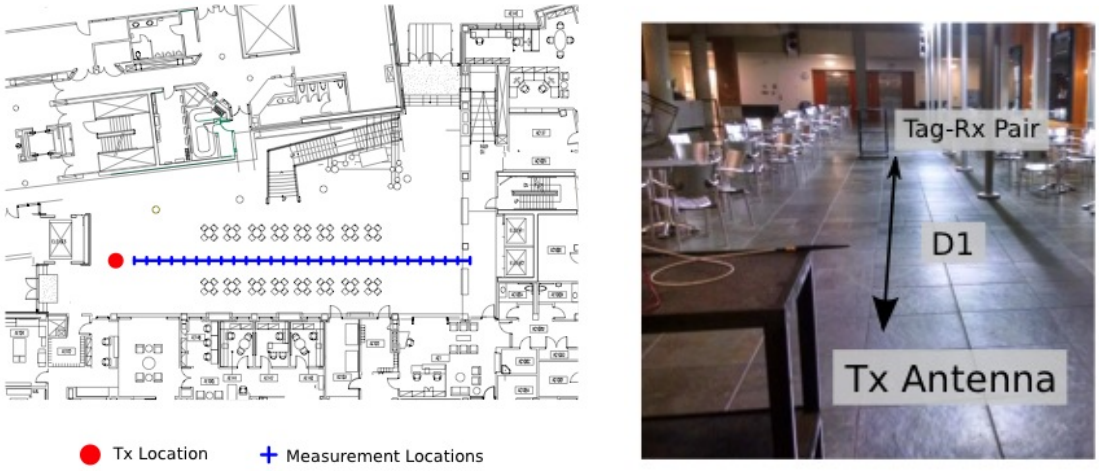
Fig. 8.9(b) shows the modeled SIR with a source transmit power of +16 dBm EIRP is above the measured SIR requirement for the Nordic Semiconductor nRF51822 with a 9 MHz offset frequency for all distance $D_1 + D_2$ from 0 m to 13 m. In practical applications some margin should be added to account for the effects of misalignment and multipath fading.

8.4 Mitigating Interference

8.4.1 Paired Bistatic Setup

There are two potential pairings that lead to an increased SIR at the receiver. The backscatter device and receiver can be paired, or the carrier signal source and backscatter device can be paired. An example application where the backscatter device and receiver are paired is a wearable device scenario. An example application where the carrier source and backscatter device are paired is a wireless sensor scenario.

One example application scenario for the proposed BLE-Backscatter approach is to provide a data uplink from a wearable sensor, such as a fitness tracker or a



(a) (b)

FIGURE 8.10: (a) Building floor plan used for OTA testing with measurement locations (b) Photo of OTA test setup

smart watch, to a user's smart phone or tablet. We conducted the OTA experiments to explore this scenario in a large open atrium (14 m x 40 m) in our building. To simulate this wearable sensor scenario, we fixed the distance D_2 at 1 m to represent the distance between a wearable sensor and a smart phone or tablet carried by the user. A CW source at a frequency of 2414 MHz was set up at one end of the atrium using an Agilent N5181A RF signal generator and a MiniCircuits ZHL-16W-43-S+ RF amplifier at three different power levels to yield an EIRP of +36, +26, and +16 dBm EIRP using a dipole whip antenna.

Fitness trackers or smart watches are normally powered by an internal battery to ensure continuous operation when the wearable sensor is away from other sources of energy, so this application does not require RF energy harvesting, although we considered this possibility by measuring the available RF power at the BLE-Backscatter device to determine how much RF power was available at each location. A second dipole whip antenna was connected to an Agilent N9320B spectrum analyzer to measure the available RF power from the CW source as the distance D1 was varied from

1 m to 30 m. The resulting measurements are shown in Fig. 8.11. With an RF energy harvesting sensitivity of -25 dBm, as described in [22], the distance D1 at which useful power could be harvested ranges from 8 meters for a +36 dBm EIRP source to 5 meters for a +26 dBm EIRP source.

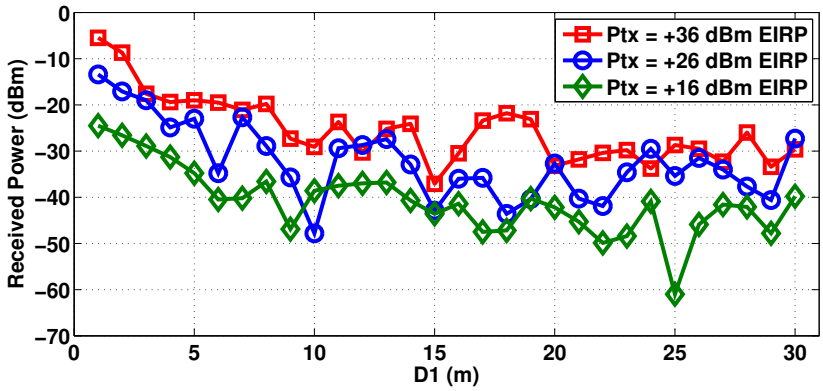


FIGURE 8.11: Measured available RF power from carrier source vs. tag distance D1

The spectrum analyzer was then disconnected and the BLE-Backscatter tag was attached to the dipole whip antenna. An unmodified Apple iPad Mini was fixed at a distance of 1 m from the BLE-Backscatter tag to simulate the wearable sensor application described above. The combination of the BLE-Backscatter tag and the iPad Mini were then moved radially away from the CW source to change the distance D_1 as above. At each measurement distance D_1 the Apple iPad Mini was rotated within a 10 cm radius to optimize the RSSI value, since the radiation pattern and polarization of the iPad Mini antenna are not specified by Apple.

The maximum observed RSSI value at each distance D_1 is plotted in Fig. 8.12. The sensitivity of the iPad Mini, as determined by the minimum RSSI at which valid packets were reported, is plotted as a black dotted line at -105 (arbitrary units). For all three of our transmitter power levels (+36, +26, and +16 dBm EIRP) we were able to successfully receive BLE packets at all of the measurement positions for D_1 = 1 m to D_1 = 30 m.

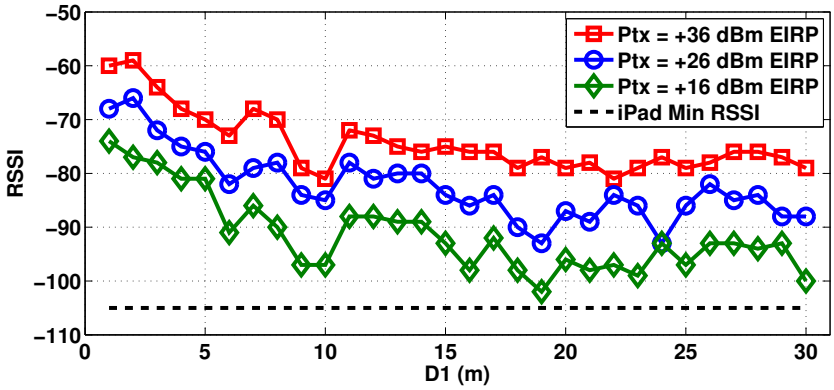


FIGURE 8.12: Measured maximum reported RSSI (arbitrary dB units) with a fixed 1 m separation between iPad Mini and BLE Backscatter tag

8.4.2 Monostatic carrier cancellation

One challenge in most backscatter communication systems is that the receiver must demodulate the desired, relatively weak, backscattered signal in the simultaneous presence of the carrier, which is usually much stronger and thus prone to desensitize the receiver. In a backscatter system, the interfering carrier is often called a *self-jammer*.

The use of unmodified, standard wireless receivers (e.g., a Bluetooth chipset) in backscatter systems was first demonstrated in [3]. The same approach has since been shown to also work with Wi-Fi and Zigbee communication standards [103]. To date, these implementations have used two-antenna bistatic configurations where the carrier source is physically separated from the receiver. The bistatic configuration has the advantage of reducing self-jamming at the receiver caused by the carrier source. In this section, we consider a single-antenna, monostatic approach where the carrier source and the receiver share a single antenna as shown in Fig. 8.13.

The system permits the co-location and simultaneous operation of a commercial Bluetooth chipset with a carrier source, enabling the use of specially designed BLE-Backscatter tags to send data to the commercial Bluetooth chipset with no

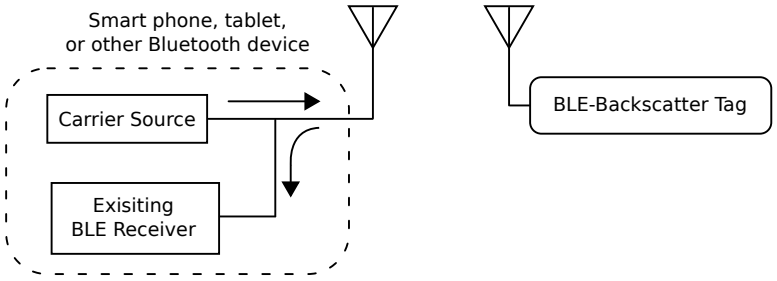


FIGURE 8.13: Backscatter reader using a commercial off-the-shelf BLE receiver

software modifications. This demonstration shows the potential for reusing the wireless chipsets in future full-duplex devices as readers for backscatter tags and other backscatter-based devices. We leverage the properties of a directional coupler with a mismatched port to provide significant ($\geqslant$ 50 dB) cancellation of the self-jamming carrier at the receiver port. This approach is similar to that used in some UHF RFID readers [112, 113]. We believe that this architecture also has other benefits in future full-duplex wireless communication systems, because self-jammer cancellation will likely be needed in future smart phones, mobile devices, and access points implementing full-duplex operation [114, 115, 116]. As full-duplex devices become commercially viable, they will likely already have a majority of the hardware required to function as backscatter readers with the specially designed backscatter tags described in [3, 103]. Thus we see the development of full-duplex wireless hardware as a potential boon for interoperation with backscatter tags and other backscatter devices.

Monostatic Link Budget

A monostatic link budget was constructed to estimate the strength of the backscattered signal from the BLE-Backscatter tag in a free-space propagation environment. A detailed description of the BLE-Backscatter tag used in this section can be found in Chapter 6. The backscattered power available from the tag is

$$P_{tag} = \frac{P_t G_t \Delta\sigma}{4\pi R^2} \tag{8.12}$$

where R is the distance from the carrier source (and co-located receiver) to the tag, P_t and G_t are the carrier power and gain of the transmitting antenna respectively, and $\Delta\sigma$ is the differential radar cross section (RCS) of the tag [102, 83] given by

$$\Delta\sigma = \frac{\lambda^2}{4\pi} G_r^2 \left|\Gamma_1^* - \Gamma_2^*\right|^2 \tag{8.13}$$

where G_r is the gain of the tag antenna and Γ^* is the conjugate match reflection coefficient

$$\Gamma^* = \frac{Z_a^* - Z_L}{Z_a + Z_L} \tag{8.14}$$

for a resonant antenna impedance Z_a and the complex load impedance Z_L.

The power received at the reader is

$$P_{Rx,BLE} = \frac{P_t G_t^2 \Delta\sigma \lambda^2}{(4\pi)^3 R^4} \tag{8.15}$$

Parameters for the link budget calculations are shown in Table 8.4. The reader and tag antennas are standard whip dipoles with 2.1 dBi gain. Values for Z_{L1} and Z_{L2} were measured with an Agilent N5222A PNA network analyzer over the 2400 MHz to 2483 MHz band at the SMA port of the BLE-Backscatter tag. The values of Z_{L1} and Z_{L2} at 2414 MHz were used in our link budget table since that is the carrier frequency used for this demonstration.

Monostatic Carrier Cancellation

The carrier cancellation architecture shown in Fig. 8.14 uses the properties of a directional coupler to suppress the self-jamming carrier at the receiver's input port.

Table 8.4: Parameters for monostatic link budget calculation

λ	0.124 meters
P_t	+33.9 dBm
G_t, G_r	2.1 dBi
Z_a	50 + j 0 Ω
Z_{L1}	76 - j 74 Ω
Z_{L2}	78 + j 93 Ω

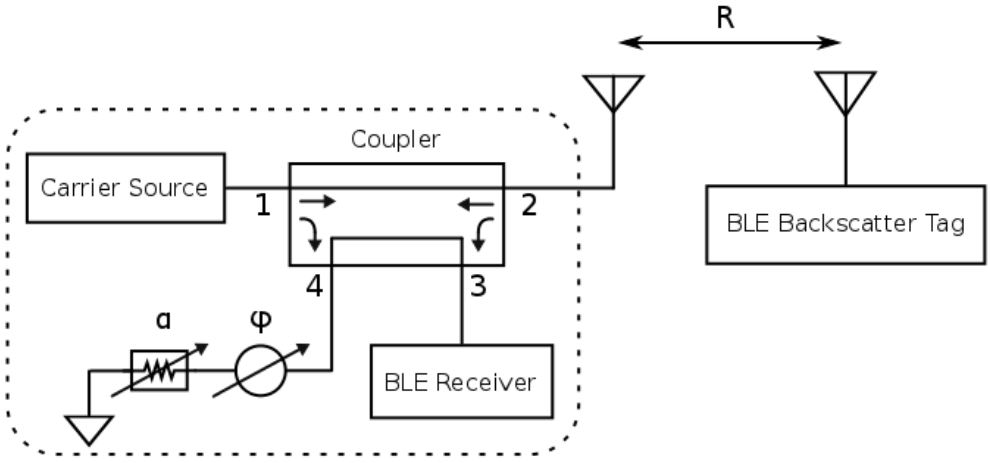


FIGURE 8.14: Full-duplex backscatter system block diagram showing carrier cancellation network

The scattering matrix (S) defining the four port network of the directional coupler is

$$S = \begin{vmatrix} 0 & S_{12} & S_{13} & S_{14} \\ S_{12} & 0 & S_{23} & S_{24} \\ S_{13} & S_{23} & 0 & S_{34} \\ S_{14} & S_{24} & S_{34} & 0 \end{vmatrix} \tag{8.16}$$

For the purpose of analysis, we assume the coupler is terminated in perfect 50 Ω impedances at ports 1 and 3 by the carrier source and receiver respectively. Port 2 is connected to an antenna with a non-ideal return loss. Port 4 is connected to a reflective termination (short) via a variable phase shifter and attenuator with α dB of attenuation. The voltage seen at port 3, the receiver, is then a combination of the

signals from ports 1 and 2:

$$\begin{aligned} V_3 =& V_1 S_{31} + V_1 S_{21} \Gamma_{2A} S_{32} + V_2 S_{32} + \\ & [V_1 S_{41} + V_2 S_{42}] S_{34} (10^{\alpha/20})^2 \angle (2\phi + 180^o) \end{aligned} \tag{8.17}$$

where V_1 is the voltage from the carrier source, V_2 is the received voltage at the antenna, and Γ_{2A} is the reflection coefficient at port 2 of the coupler going in the antenna. The term $V_1 S_{31}$ in Eq. 8.17 occurs because the isolation between the carrier source at port 1 and the receiver at port 3 of the coupler is not perfect. Additionally, there is some impedance mismatch between the output of the coupler at port 2 and the antenna. The reflected power from the antenna (forming the self-jammer), along with the desired backscatter signal, is coupled into the receiver at port 3.

Monostatic carrier cancellation results

In our experiments, we used a Mini-Circuits ZABDC20-252H-S+ directional coupler, an Aeroflex 980-2K phase shifter (340 degrees phase shift range), and a JFW Industries Inc. 50R-019 step attenuator (0-10 dB attenuation, 1 dB step size). As shown in Fig. 8.15, the dipole antenna used in our over-the-air testing is relatively well matched, having a return loss of 20 dB at the selected carrier frequency of 2414 MHz.

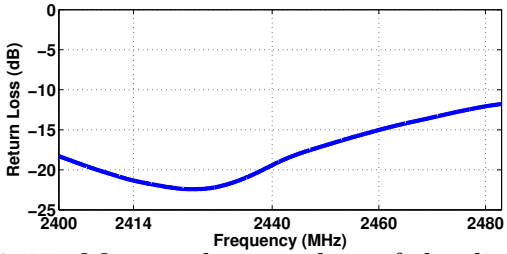
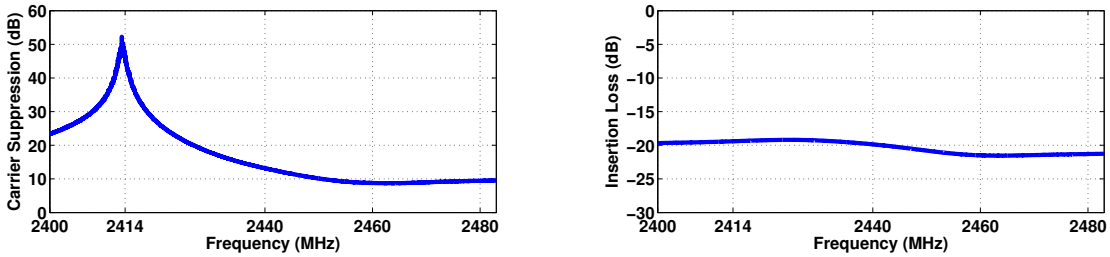


FIGURE 8.15: Measured return loss of the dipole antenna

By terminating the antenna port (port 2) of the directional coupler with a 50 Ω load, and using an Agilent N5222A PNA network analyzer, we were able to measure

the self-jammer power received at port 3 from the carrier source (port 1). This is the baseline self-jammer power due to the coupler's directivity. When we attached the actual antenna at port 2 and manually tuned the attenuation, α, and phase, ϕ, at port 4, we received another measurement for the self-jammer due to reflection from the antenna.



(a) (b)

FIGURE 8.16: (a) Measured carrier suppression at 2414 MHz (b) Measured insertion loss of the carrier cancellation network, antenna to receiver input port

By taking the difference of return losses when there is a 50 Ω terminator vs. with the actual dipole antenna, we can calculate the suppression of the antenna-reflected self-jammer. As shown in Fig 8.16a., we achieve 50 dB carrier suppression at our designated carrier frequency of 2414 MHz. We observe a 3 dB suppression bandwidth of 1 MHz.

This suppression comes at a cost, of course. Since we used a 20 dB directional coupler, we expect to observe a 20 dB reduction in the backscatter tag signal at the receiver port. This is confirmed by the measurement shown in Fig. 8.16b.

Monostatic over-the-air test results

To test the performance of our monostatic BLE-Backscatter reader we performed over the air (OTA) measurements with a Nordic Semiconductor nRF58122 evaluation board acting as our BLE receiver. The carrier source was an Agilent N5181A signal

generator, amplified by 45 dB using a Mini-Circuits ZHL-16W-43-S+ RF amplifier to achieve an output power of +33.9 dBm.

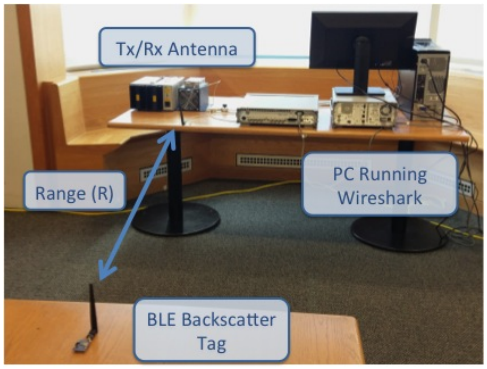
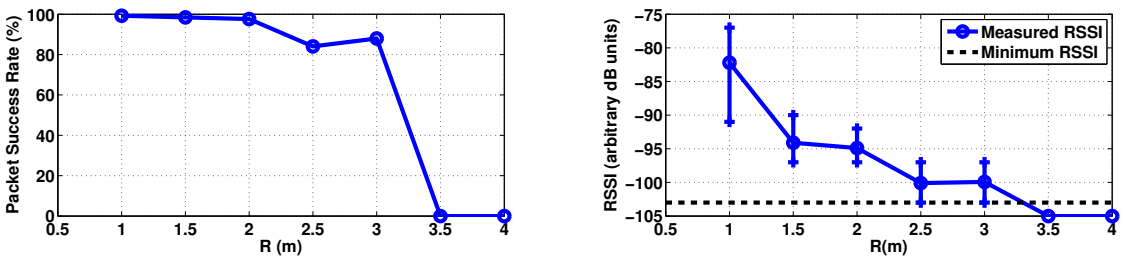


FIGURE 8.17: Photo of monostatic test setup

The distance R from the backscatter tag to reader was moved in 0.5 m steps from 1 to 4 m and at each location the carrier cancellation circuit was adjusted to minimize the received carrier power. While this adjustment was performed manually in our test setup, a commercial version of this architecture would include automatic tuning of the carrier cancellation circuit. A photo of this test setup is shown in Fig. 8.17. At each measurement location, 10,000 backscatter packets were transmitted and the number of successfully received packets was recorded using Wireshark, an open source packet analyzing tool. The packet success rate as a function of range from the tag to reader is shown in Fig. 8.18a.

The received signal strength indicator (RSSI) values provided by the Nordic Semiconductor chipset were also recorded at each measurement location. These RSSI values are reported by the chipset in arbitrary log units (dB), rather than being well-calibrated relative to any reference power. When the BLE-Backscatter tag is within 3 meters of the co-located carrier source and receiver, over 80% of the transmitted backscatter packets are received with zero bit errors. Beyond 3 meters no packets were received successfully. The maximum range of the reader appears to be limited by the receiver sensitivity of the Nordic Semiconductor nRF58122 evaluation



(a) (b)

FIGURE 8.18: (a) Packet success rate as reported by Wireshark (b) RSSI values reported by Wireshark

board. The minimum RSSI value observed for successfully received packets is −103 (arbitrary units). As shown in Fig. 8.18b. the observed RSSI values for measurements at 2.5 and 3 meters are just above the minimum RSSI threshold, with average RSSI values near -100. Future work will consider implementing an automated adaptive carrier cancellation circuit that will automatically minimize the self-jammer power as the antenna return loss changes. A directional coupler with increased coupling (e.g. 10 dB) will be considered rather than the 20 dB coupler used here.

8.4.3 Frequency Diversity

Transmitting OTA messages using frequency diversity is a technique for dealing with the negative influence of destructive interference and narrow band interferers. To overcome the possibility of transmitting at a frequency that is already being used by another transmitter, or transmitting at a frequency that results in a multipath null at the receiver many communication schemes will transmit simultaneously or sequentially at multiple frequencies. One reason why the BLE frequency plan has three advertising channels is to provide three different opportunities for an advantageous channel and to establish a connection between a central and peripheral device. The BLE advertising channels are spaced out in the 2.4 GHz ISM band at channels centered at 2402 MHz, 2426 MHz, and 2480 MHz. These frequencies were chosen

in part to avoid interference from the 3 non-overlapping Wi-Fi channels 1,6, and 11, centered at 2412 MHz, 2437 MHz, and 2462 MHz respectively.

As mentioned earlier in Section 7.3, backscatter messages can be designed for any of the BLE advertising channels with a single frequency carrier source. Creating messages for all three advertising channels reduces the likelihood that a multi path null will make successful reception impossible.

8.4.4 Chapter Conclusion

Limiting factors for operating BLE-Backscatter devices are explored for monstatic and bistatic setups. A characterization of a commercially available BLE receiver is conducted to understand the performance limits of a BLE-Backscatter system. The characterization focuses on the receiver sensitivity and interference rejection performance of the receiver, both of which influence the achievable communication distance. Interference mitigation techniques are explored and implemented for monostatic and bistatic systems. In the monostatic setup a range of 3 m is achieved by implementing a carrier suppression circuit. A range of greater than 30 m is demonstrated for the bistatic setup where the receiver and BLE Backscatter devices are in a physically paired configuration.

Chapter 9

A Low Power BLE Receiver Using an External LO Source

9.1 Introduction

This chapter focuses on a wireless receiver topology for sensors and mobile devices that consumes less power than conventional architectures while retaining compatibility with existing wireless standards used by mobile devices. The work described in Chapters 6-8 concerned a low power uplink using backscatter modulation to communicate with existing unmodified BLE receivers. Here we explore an approach to receive BLE signals that takes advantage of an externally generated local oscillator (LO). The proposed device leverages the same carrier source and antenna to perform three distinct operations. The three operations are energy harvesting, backscatter modulation, and demodulation using an externally generated LO.

A block diagram of a receiver using an external LO can be seen in Fig. 9.1. Both the desired wireless signal and external carrier source are received by the same antenna and jointly fed to a specially designed two-port mixer. A low power receiver that uses an external carrier source can leverage the same carrier used in the

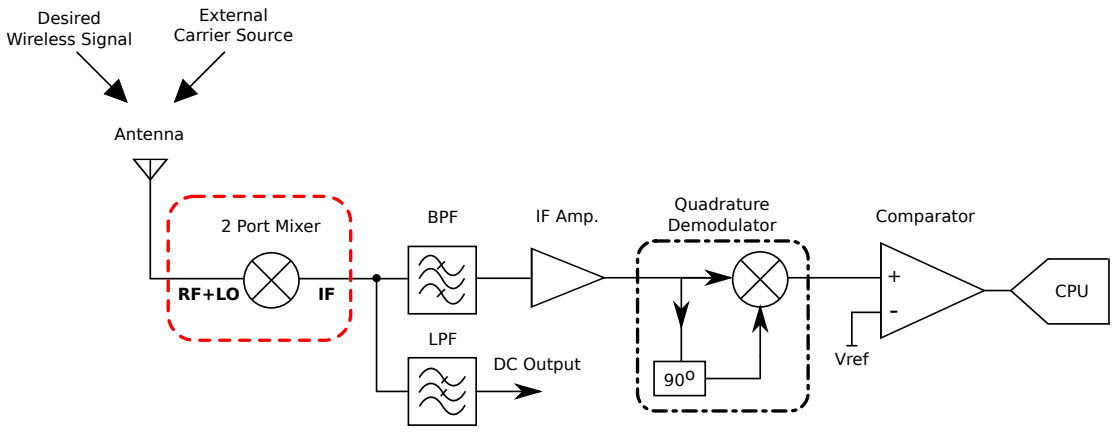


FIGURE 9.1: Simplified receiver block diagram

backscatter technique that was previously described in Chapters 6-8. Both the uplink using BLE-Backscatter and downlink using our low power receiver architecture leverage an external carrier source to reduce the energy expenditure of generating an on-board (or on-chip) LO. Characterization of the receiver includes an evaluation of the specially designed two-port mixer for its low LO input power performance. A measured conversion loss of 27 dB is observed for the two-port with an RF input power of -20 dBm and an LO input power of -20 dBm. In a cabled, bench top test, successful reception of BLE messages is achieved with zero bit errors using a Matlab decoder with an RF input power of -8 dBm and an LO input power of 3 dBm.

9.2 External LO Approach: Two-Port Mixer

For conventional receivers, LO generation is a significant energy expenditure. Creating a precise high frequency LO typically involves a power hungry PLL circuit. Our receiver topology, as shown in Fig. 9.1, offloads the LO generation to the external carrier source described in Fig. 1.1. The receiver takes the LO from the carrier source and RF from a transmitter, such as a smart phone transmitting BLE signals, and uses them as the input to a "two-port mixer". In conventional frequency mixers there are usually three ports: one each for the LO input, RF input, and IF output

signals. In the two-port mixer described here, the LO and RF inputs are received simultaneously on the same antenna and jointly fed into the first port of the mixer. The IF output port contains energy at the sum and difference frequencies between the LO and RF frequencies. The LO signal may be a higher frequency than the desired wireless signal (high-side injection) or a lower frequency than the desired RF signal (low-side injection). A frequency domain illustration of the two-port mixer operation is shown in Fig. 9.2. The data-carrying RF signal is translated in frequency from the carrier frequency down to a much lower IF frequency for filtering and demodulation. In the case where the desired RF signal is a BLE message the frequency translation is from the 2.4 GHz ISM band down to a desired IF frequency. The choice of IF frequency could include traditional IF frequencies such as 455 kHz, 10.7 MHz, 45 MHz, or 100 MHz.

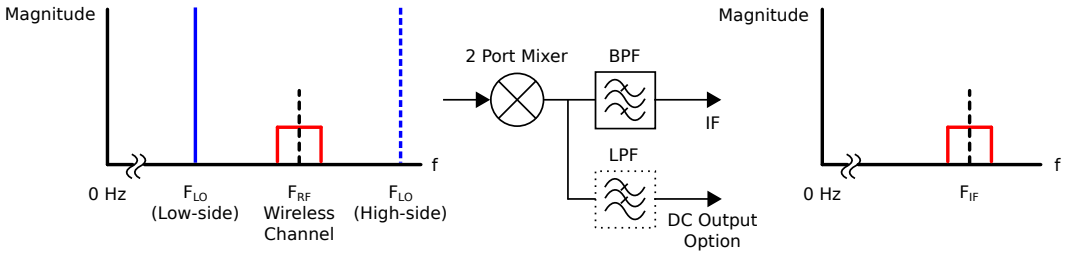


FIGURE 9.2: BLE receiver mixing concept

After mixing, a band pass filter is used to reject unwanted mixing products and leave only a baseband version of the transmitted BLE signal. The baseband signal is then amplified to bring it to a useful power level for demodulation. Since the BLE transmission is an FSK signal, two options for demodulation are a discriminator circuit or I/Q demodulation of the IF signal. The demodulated outputs are then fed into a comparator to digitize the BLE waveform. For our proof of concept prototype decoding packets is performed by a CPU running Matlab following the specifications for BLE advertising packets.

We describe an optional DC output where the DC component of the mixer output is used as a power source for the receiver or other circuitry. Depending on the operation of the tag the harvested DC output and IF output can either be used simultaneously or independently. In low duty cycle applications the DC output would be harvested over a long period of time to accumulate enough energy to operate the IF demodulator.

9.3 Mixer Design and Characterization

Diode based mixers have been used for decades for their frequency conversion properties [117, 118, 119, 120]. An example single diode mixer is shown in Fig. 9.3. The diode is presented with two inputs, an LO and RF input and the resulting output frequencies contain the sum and difference frequencies of the LO and RF inputs.

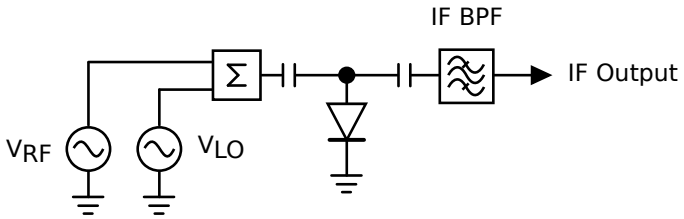


FIGURE 9.3: Single diode mixer

For a simplified explanation of how diode based mixers produce mixing products we can think of the LO signal changing the resistance or conductance of the diode that is seen by the RF signal. The time-varying conductance can be written as

$$g(t) = G_0 + G_1 \ cos(\omega_{LO} \ t) \tag{9.1}$$

and the time-varying RF voltage can be written as

$$V_{RF}(t) = V_{RF} \ cos(\omega_{RF} \ t) \tag{9.2}$$

The resulting time-varying current is then

$$i(t) = g(t)V_{RF} \ (t) \tag{9.3}$$

$$i(t) = G_0 V_{RF}\, cos(\omega_{RF}\, t) + \frac{1}{2} G_1 V_{RF}\, [cos(\, (\omega_{RF} - \omega_{LO})\, t) + cos(\, (\omega_{RF} + \omega_{LO})\, t)] \quad (9.4)$$

The time-varying current from equation 9.4 contains frequency components at both the sum frequency $\omega_{RF} + \omega_{LO}$ and difference frequency $\omega_{RF} - \omega_{LO}$. For our receiver we will use the difference frequency and filter out the other mixing products with an IF band pass filter.

Our designs have focused on diode based two-port mixers. An important element in the design of the mixer is a matching network to maximize the total power transfer from the received signal at the antenna to the input of the mixer. For accurate modeling of the matching network for a nonlinear device, a choice of input power is required. As an initial estimate of the expected input power to the mixer, Fig. 9.4 shows the expected received power from a +23 dBm EIRP carrier source plotted with a solid blue line and a +10 dBm EIRP BLE source plotted with a dashed green line. The +10 dBm EIRP BLE transmission is the maximum output power specified for Bluetooth Low Energy transmitters in the Bluetooth specifications [45]. For situations where the receiver is near the carrier source (e.g. within 2 meters from a +23 dBm EIRP source) a reasonable target power level for RF matching is -20 dBm. This target input power level is also reasonable given the measured data from Fig. 8.11 showing the received power at distances of 1 m to 30 m with transmit powers of +36, +26, and +16 dBm EIRP.

The design of the two-port diode mixer and RF matching circuit was performed using AWR Microwave Office. Avago HSMS-286C Schottky diodes were selected for their high frequency, low power performance. To properly simulate the HSMS-286C diodes, both the diode model and package model must be included in the simulation [121, 122]. The design uses a microstrip matching network for RF matching and a lumped element matching network for IF matching, as illustrated in Fig. 9.5(a) The RF matching is designed for a 50 Ω system for convenient cabled testing and use with

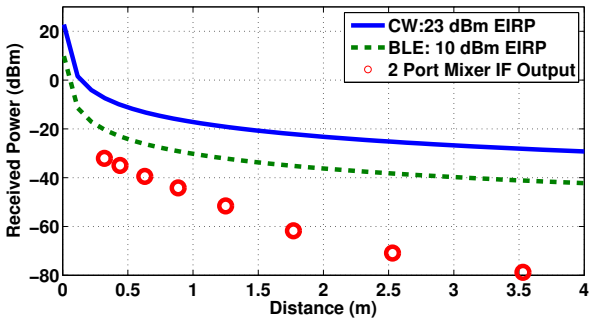


FIGURE 9.4: Estimated received power from a +23 dBm ERIP carrier source and a +10 dBm EIRP BLE source

50 Ω antennas. The RF matching network was optimized for an input power level of -20 dBm. A Rogers 4003C substrate was used to minimize losses in the microstrip matching network.

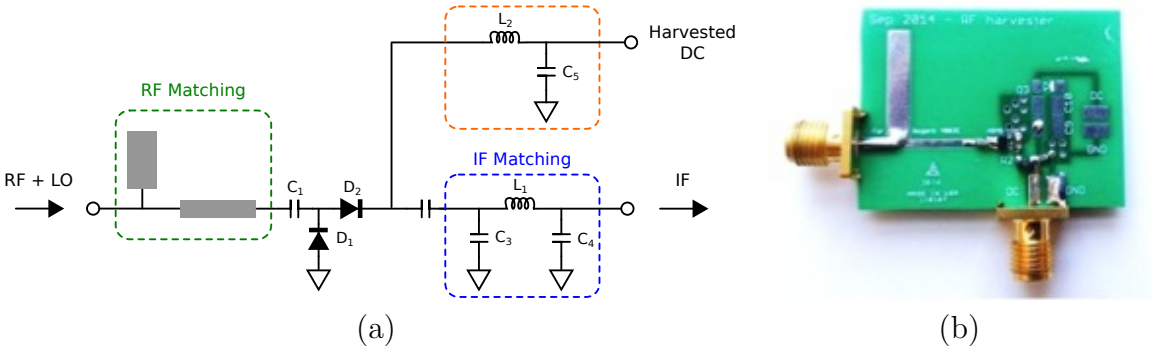


FIGURE 9.5: (a) Diode based two-port mixer block diagram (b) Photo of two-port mixer including distributed element RF matching and lumped element IF matching

A photo of the fabricated and populated two-port mixer is shown in Fig. 9.5b. The microstrip matching network is on the left of the board directly after an SMA connector input for the RF and LO signals. The Avago HSMS-286C diodes are near the center of the board. The bottom right hand corner shows the lumped element matching network leading to the SMA output connector.

Characterizing the performance of the fabricated two-port mixer required using a network analyzer for RF matching measurements and the cabled test setup in Fig. 9.6

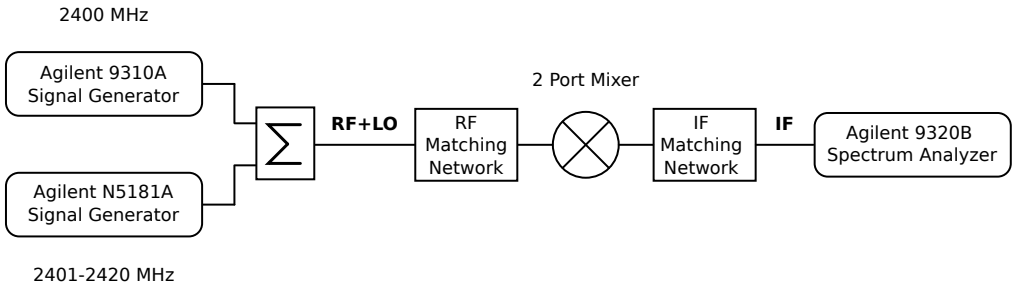
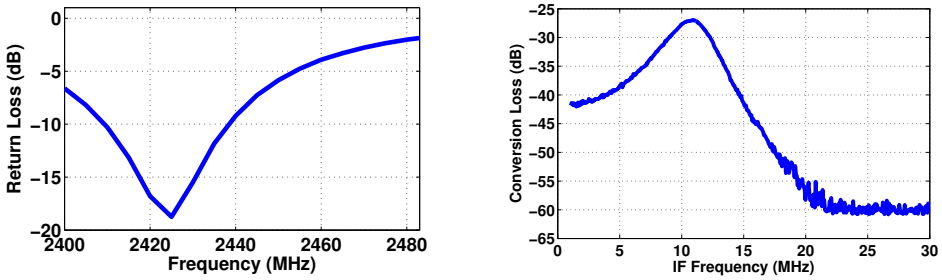


FIGURE 9.6: Cabled test setup for mixer conversion loss testing

for conversion loss measurements. The input return loss shown in Fig 9.7(a). was measured with an Agilent N5222A PNA network analyzer with a measurement power of -20 dBm. A good matching performance is observed for our desired frequency range near BLE channel 38 at 2426 MHz.



(a) (b)

FIGURE 9.7: (a) Measured return loss of two-port mixer (b) Mixer conversion loss vs. frequency, P_{LO} = -20 dBm, P_{RF}: -20 dBm

The mixer conversion loss shown in Fig. 9.7(b) was measured with RF and LO input powers of -20 dBm. Mixer conversion loss is reported with reference to the RF input power. At 10.9 MHz, when the conversion loss is at its minimum, the IF power at the spectrum analyzer is -47 dBm, for a conversion loss of 27 dB with respect to the initial RF input power. Fig. 9.7(b) shows the importance of the IF matching network. The IF frequency response is matched to our desired frequency range, 9 - 11 MHz and provides significant rejection of higher frequency mixing products prior to the BPF.

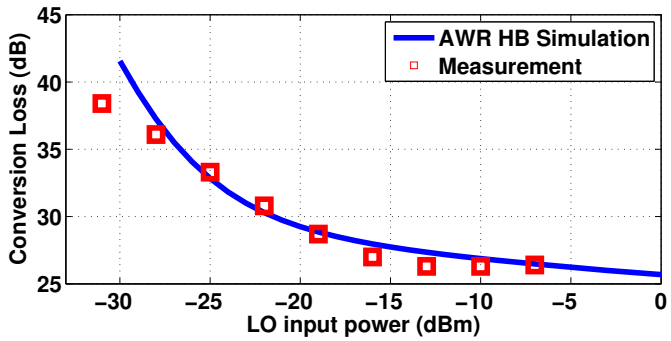


FIGURE 9.8: Mixer conversion loss measurements and simulation, $P_{LO} = P_{RF}$

To measure the conversion loss as a function of input power, a single frequency is used for the LO and RF source of 2400 and 2411 MHz respectively. Measurements were again performed with the cabled test setup described in Fig. 9.6. A comparison between measured results and AWR Microwave Office harmonic balance simulations is shown in Fig. 9.8. For these measurements the conversion loss is listed as a function of RF input power.

A constraint when relying on an external LO is that the receiver architecture described in this chapter requires operation with a wide range of LO and RF input powers. The input power of the mixer is dependent on the transmit power and range to the receiver from the desired wireless transmission source and carrier source. When the LO is generated onboard the receiver, an optimized, known LO input power can be used to drive the receiver's mixer at the cost of using energy to generate the required high frequency LO signal. Our alternative architecture requires an external LO source and must be able to operate with uncertain input power levels of the LO and RF data carrying signals. Use cases for this receiver architecture will depend on the useful range of LO and RF input powers expected from the carrier source and source of the desired wireless signal. For the range of input power between -7 dBm and -31 dBm there is good agreement between measured and simulated conversion loss.

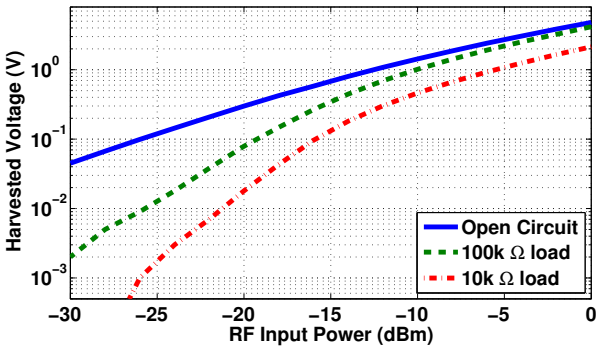


FIGURE 9.9: Measured DC output voltage from two-port mixer

To test the DC output of the two-port mixer a cabled test was performed using a single CW input to the mixer with a voltmeter measuring the harvested DC voltage. An Agilent N9310A signal generator producing a CW signal at 2400 MHz was used. As shown in Fig. 9.9 the harvested voltage was collected between input power levels from -30 to 0 dBm. The harvested voltage was measured with an open circuit output, with a 100 kΩ load, and with a 10 kΩ load. Depending on the voltage and power requirements of the receiver and backscatter transmitter this DC output can be used directly or with a DC-DC boost converter like the one described in Chapter 5.

9.4 Bench top testing of complete receiver

Key elements of the receiver architecture were tested with a cabled bench top test setup shown in Fig. 9.10. A Nordic Semiconductor nRF24LO1+ transceiver is used to generate a repeatable source of known BLE transmissions. The BLE transmissions represent the desired wireless signal. All BLE transmissions are in advertising channel 38, which has a center frequency of 2426 MHz. The total duration of the BLE transmission is 232 μs and the transmissions are repeated once every 140 ms. The LO signal of 2415 MHz is provided by an Agilent N9310A signal generator. The 2415 MHz LO signal is continuously present. The LO signal and BLE signal are combined with a Mini-Circuits ZN2PD2-63-S+ power splitter and are then fed into

the input port of the two-port mixer. In an OTA test these signals would be received simultaneously by the antenna and fed to the two-port mixer.

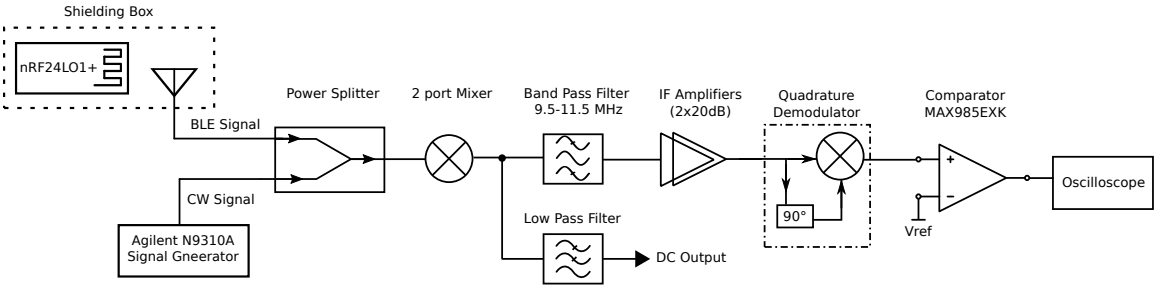


FIGURE 9.10: Block diagram of cabled receiver test setup

The band pass filter shown in Fig. 9.10 is a three pole Butterworth band pass with cutoff frequencies of 9 and 13 MHz implemented with lumped element capacitors and inductors. In the bench top test setup we use two IF amplifiers in cascade. Both are Mini-Circuits ZFL-550+ amplifiers with individual gains of 20 dB resulting in a total IF gain of 40 dB. The quadrature demodulator consists of a Mini-Circuits ZFY-1-S+ mixer and phase shifter circuit. The output of the quadrature demodulator is connected to a MAX985EXK comparator where the demodulated data is digitized. The digitized output of the comparator is connected to an oscilloscope to view the resulting waveform.

Fig. 9.11 shows a photo of the cabled receiver test setup. Two DC power supplies are used, one to power the IF amplifiers and another to power the MAX985EXK comparator. The two cables going into the power splitter are coming from the RF signal generator and the shielding box containing the Nordic Semiconductor nRF24LO1+ transceiver. A shielding box was used to prevent interference from nearby BLE-enabled smart phones transmitting on Ch. 38. The oscilloscope pictured on the right shows a full BLE packet captured using the oscilloscope. Raw sampled data from the oscilloscope are saved to a USB stick as .csv files and decoded offline

on a PC running Matlab.

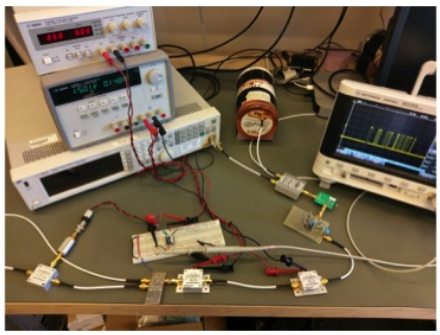


FIGURE 9.11: Photo of cabled receiver test setup

To determine if the receiver and Matlab decoder are functioning properly, without introducing bit errors in the received packets, a known BLE advertising packet is repeatedly transmitted by the Nordic Semiconductor nRF24LO1+ BLE signal source. The packet used to test the low power receiver has a total packet length of 232 bits and is shown in Fig. 9.12(b). The preamble and access address are fixed for BLE advertisement messages. The payload data unit (PDU) contains information for the length of the total packet and the device name. In this case "BLE-MBS!" is used.

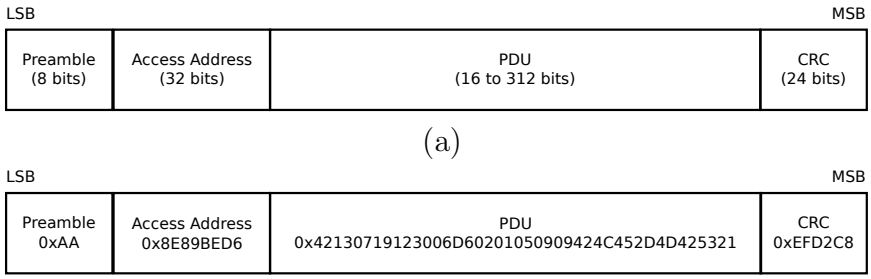


FIGURE 9.12: (a) BLE packet format (b) example packet bit string with device name "BLE-MBS!"

To verify the "ground truth" of the known packet, for BLE transmissions from the nRF24LO1+ transceiver both an Apple iPad mini and nRF51822 evaluation board were used. The Apple iPad mini showed packets with the desired device name

"BLE-MBS!". The full packet information was also verified with data collected from Wireshark using a Nordic Semiconductor nRF51822 evaluation board.

Fig. 9.13 shows the known transmitted BLE signal on the top plot and a saved data file of a received packet from the oscilloscope on the bottom plot. The start of the received packet was determined using a correlation with the known 8 bit preamble. The total length of the packet was determined by the length field in the PDU. The bottom plot shows output voltages from the comparator at either 0 V or 2.3 V representing a digital zero or one. The total plotted time is from 0 to 232 μs, the full length of the BLE advertisement packets used in this test. Both plots in Fig. 9.13 show four gray boxes indicating the time intervals for the preamble, access address, PDU, and CRC.

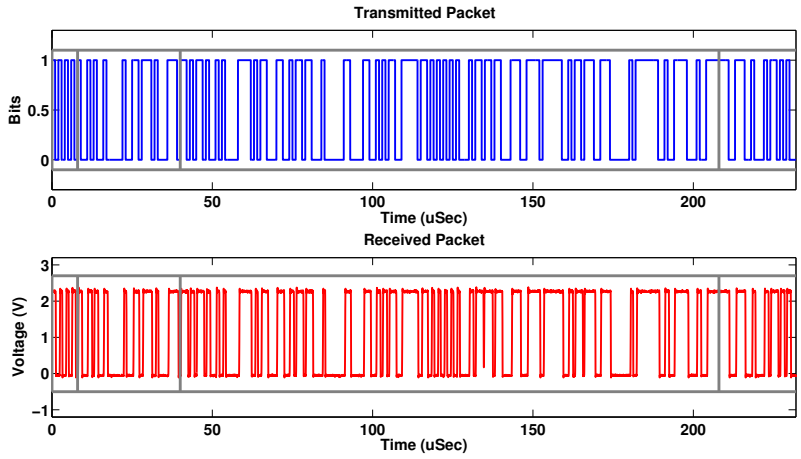


FIGURE 9.13: Demodulated Packet

Fig. 9.14 shows the Matlab decoding of the preamble and access address portion of the BLE advertising packet. The first 8 bits of the advertising packet are the preamble and the next 32 bits are the access address. These 40 bits are always the same for BLE advertising packets. Once the received signal has been digitized to decode the preamble and access address, the bits have to be grouped into bytes with the least significant bit first, meaning the first bit to arrive at the receiver is

the least significant bit of each byte. Once the received data stream is grouped into bytes, both the preamble and access address are interpreted with the least significant byte having been transmitted first. These operations are shown in Fig. 9.14 and the required information for decoding the remaining section of the BLE advertising packet is explained in [45].

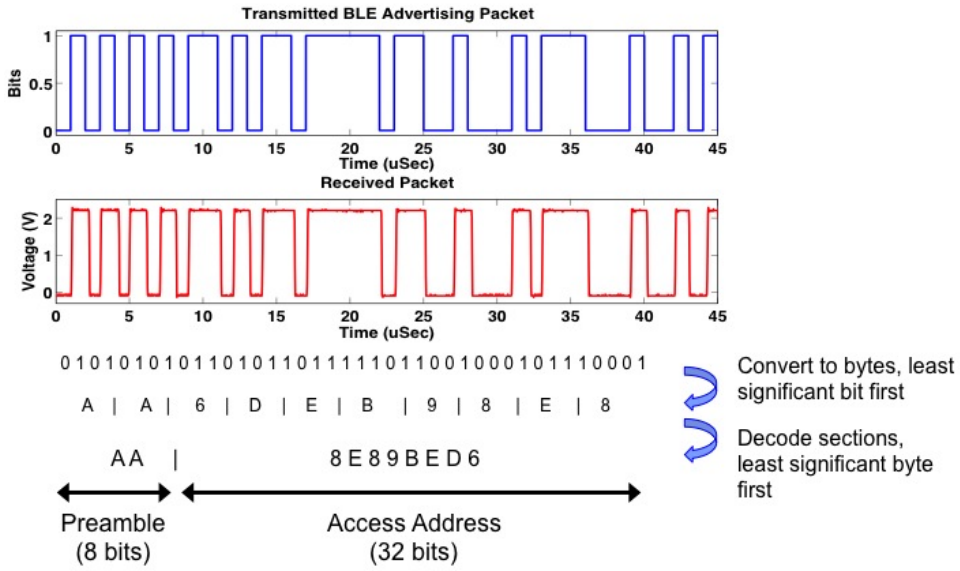


FIGURE 9.14: Decoded Preamble and Access Address

9.5 Performance Characterization

In our bench top cabled test setup successful demodulation and decoding has been performed with a BLE advertising channel input power of -8 dBm and a CW carrier input power of 3 dBm into the two-port mixer. These minimum input power levels are higher than would be expected in OTA testing.

Improvements to the receivers are required before OTA testing can take place. The current frequency plan has an IF frequency centered at 11 MHz. The BLE signal of interest uses a GFSK modulation scheme with binary frequencies of $\pm$ 250 kHz. Lowering the IF center frequency would result in a more sensitive quadrature de-

modulator resulting from a greater phase difference caused by the 90^o phase shifter designed for one of the two modulation frequencies.

The greatest source of losses in the receiver come from the two-port mixer which has a measured conversion loss of 27 dB with RF and LO input powers of -20 dBm. New designs to minimize the conversion loss of the mixer would also decrease the minimum required input power of the receiver. A low power active mixer could be considered as an alternative to the lossy diode mixer.

9.6 Chapter conclusion

We have validated a low power BLE receiver architecture using an external LO source with a custom designed passive two-port mixer and functional testing blocks from Mini-Circuits. This receiver architecture takes advantage of an externally generated LO and removes the requirement for onboard LO generation. It has a measured sensitivity of -8 dBm with a CW source power of +3 dBm. Remaining work on this low power receiver includes a consideration of an active diode based or FET based two-port mixer. Switching from a passive mixer to an active mixer design will increase the power consumption of that portion of the receiver but with a significant potential savings in the mixer conversion loss at low LO input powers.

Chapter 10

Conclusion and Future Work

This document has presented new wireless power and communication architectures for ultra-low-power wireless sensors and other devices such as wearables. We consider the benefits of having a carrier present in the environment for ultra-low-power applications. The external carrier provides benefits for three distinct operations: RF energy harvesting, a backscatter based low power data uplink, and a data downlink that does not require on board (or on chip) local oscillator (LO) production.

Harvesting RF energy from both ambient and dedicated RF sources is considered in this document. An approach for characterizing and measuring the amount of RF energy in an environment is presented along with an analysis of the useable energy that can be harvester from ambient sources. RF harvesting approaches using a DC-DC boost converter to generate a useable voltage level are demonstrated using a 2.4 GHz CW carrier source with an input power level of -15 dBm.

This work expands the applicability of backscatter based devices beyond operation only with specialized infrastructure (e.g. RFID readers). We demonstrate that communication systems for energy constrained devices can be designed for MBS

without requiring a dedicated reader infrastructure. With an external carrier source a backscatter tag can generate a 1 Mbps backscatter signal that is indistinguishable from a conventional BLE transmission from the point of view of a BLE receiver.

For wireless sensors or beaconing devices that are mainly focused on transmitting data, BLE-Backscatter offers a means of significantly reducing their communication energy requirements. This could result in longer battery lifetime of current devices and it also opens up the possibility for completely new applications that were once thought of as being too energy intensive. We show that this data uplink approach can communicate with BLE receivers with a radio communication efficiency of 28.4 pJ/bit. This is over 100x lower energy per bit than conventional BLE transmitters. With off-the-shelf components, we've demonstrated communication with standard BLE receivers with a 6X reduction in energy consumption compared to conventional, active BLE transmitters. The microcontroller based BLE-Backscatter tag presented here consumes just 1.56 nJ/bit while maintaining compatibility with the billions of existing BLE receivers in smart phones, tablets, and BLE enabled devices.

Using a commercially available BLE receiver we have investigated the carrier signal requirements for generating backscatter messages. With BLE receivers we have observed that both unmodulated and modulated carriers can be used with our BLE-Backscatter tags to transmit data to unmodified BLE receivers. The use of conventional BLE transmissions as a carrier source for BLE-Backscatter tags has also been presented. Factors limiting the range of these backscatter communication techniques have been investigated for bistatic and monostatic configurations. The effect of self-jamming with the external carrier source has been characterized and interference mitigation strategies have been presented. An achieved communication range of 3 m in a monostatic configuration and 30 m in a bistatic configuration have been demonstrated.

A BLE receiver has been shown in a cabled bench top test to validate an architec-

ture using an external LO source. The receiver uses the same external carrier source leveraged to generate backscatter messages for the receiver's initial frequency down-conversion stage. In a cabled, bench top test, successful reception of BLE messages is achieved with zero bit errors using a Matlab decoder with an RF input power of -8 dBm and an LO input power of 3 dBm.

10.1 Original Contributions

The original contributions discussed in this document include:

- Characterization of available ambient energy in the 2.4 GHz band and harvesting approaches. Published in [20, 21, 22, 23].

- An approach for powering a relatively high power sensor in burst mode at an input power level of -15 dBm at 2.4 GHz. Published in [24].

- The first approach shown to create backscatter signals that are compatible with conventional wireless communication receivers using FSK, PSK, ASK, QAM, and OFDM modulation schemes such as Bluetooth, WiFi, etc. Published in [3, 25].

- The first demonstration of backscatter communication with absolutely unmodified conventional Bluetooth Low Energy receivers (neither hardware nor firmware nor software modifications are required). Published in [3].

- A microcontroller based "BLE-Backscatter" tag that produces band-pass frequency shift keying (FSK) modulation at 1 Mbps, enabling compatibility with conventional BLE receivers. To appear in [26] and Submitted [2].

- A low power receiver approach using an external LO and two port mixer has been demonstrated in a bench top, cabled setup. To be submitted and [27].

10.2 Future Work

10.2.1 Battery-free bidirectional data link

By reducing both the transmit and receive power using backscatter communication and a low power receiver architecture, one could create a BLE transceiver device that is capable of running solely from harvested RF energy sources. The battery-free transceiver would harvest RF energy from the same carrier source used for backscatter communication. As illustrated in Fig. 9.2, the low power receiver architecture using a diode based two-port mixer can simultaneously harvest a DC output and produce an IF output. Similarly, the backscatter device shown in Fig. 6.7 can harvest RF energy while communicating by connecting the harvester as a matched impedance state. Alternatively, the battery-free transceiver could operate with a duty cycled communication capability where the device alternates between harvesting and communication. The duty cycle will depend on the amount of available RF energy. These power management schemes have been studied and used in other backscatter devices such as [123, 35].

10.2.2 Single-chip approach

We expect that a future, integrated single-chip approach could substantially improve on our power result for both the backscatter data uplink and low power receiver downlink. For example in the backscatter data uplink, using fixed-function logic to generate the outgoing bit stream would be lower power than the software based approach we used in the prototype described in Chapter 6. CMOS oscillators (such as those designed for conventional UHF RFID tags) generally have significantly lower power than the discrete bipolar oscillator that we used. Further, integration of a

CMOS RF switch for backscatter modulation would reduce the amount of power needed to drive the switch compared with the board-level pads and wires in our prototype.

10.2.3 Integration with conventional BLE transceivers

While MBS offers reduced energy consumption, the nature of using a reflected signal can reduce the effective range of a device if the physical separation from the carrier source and MBS tag are unfavorable. It is also possible that data would need to be transmitted at a time when no carrier source is available in the environment. This could be due to the increased two-way path loss of MBS or because an external carrier source is not available. In most applications, the backscatter based communication system would likely be paired with a conventional transmitter and receiver. Since BLE is the dominant choice for billions of wearable devices it makes sense to choose BLE-Backscatter and an ultra low power BLE receiver as design choices for convenient integration.

Depending on the availability of a suitable carrier signal, a device with both a conventional and BLE-Backscatter communication system could choose which method is appropriate. The goal would be to use the backscatter approach whenever possible to reduce communication costs which retaining the longer operating ranges available with conventional transmitters. Similar work has been done using a WISP device and a BLE transmitter [124]. One drawback with using a WISP and BLE transmitter is the need for a separate RFID reader and BLE reader depending on the chosen communication method. By using BLE-Backscatter only the BLE reader would be necessary for receiving either the backscatter or conventional transmissions.

For the receiver further integration could be possible since the low power receiver architecture proposed in Chapter 9 and conventional receivers both perform IF filtering and demodulation. The frequency plan for the low power receiver could be

adjusted such that the IF blocks in the conventional receiver could be used following the two-port mixer.

10.2.4 Backscatter with higher-order modulation schemes

In addition to the compatibility with BLE receivers described in this document and in [3, 2] compatibility with Wi-Fi and Zigbee has been demonstrated using backscatter transmitters [46, 103]. Backscatter with high-order modulation schemes has been demonstrated with 16-QAM [4] but required the use of a custom backscatter receiver. In the future it could be possible to create a low power backscatter transmitter that works with conventional QAM receivers.

10.2.5 Multi-antenna carrier source

Multi-antenna transmitters with some form of relative amplitude and phase control could help to maximizing power transfer to a BLE-Backscatter tag. Maximize the signal power at the MBS tag would provide significant benefits for energy harvesting as well as maximizing the LO signal when using the low power receiver. Additionally, the self-jamming interference source could be minimized at the receiving device. Prior work in [125, 126] has shown the ability to create significant nulls at desired locations with a multi-antenna transmitter. Since self-jamming is a limiting factor for bistatic BLE-Backscatter having a carrier source that could actively minimize the power of the self-jammer at the BLE receiver could greatly improve the operating range.

10.2.6 Active mixer design for increased receiver sensitivity

The low power receiver architecture described in Chapter 9 has a limited sensitivity due to the high conversion loss in the passive, diode based two-port mixer. To lower the receiver sensitivity and increase the operating range of the receiver a new lower loss mixer is required. In the future an active, diode based or FET based two-port mixer could be incorporated in the receiver. The active two-port mixer would

consume more power than the current passive two-port mixer but with a potential benefit to the overall receiver performance.

10.2.7 Closing Thoughts

This is an exciting time to be involved in low power communications as the need for new solutions is being fueled by the excitement of the emerging internet of things. I look forward to the development of future backscatter based sensor nodes and wearable devices.

Bibliography

[1] K. Gudan, S. Chemishkian, J. Hull, M. Reynolds, and S. Thomas, "Feasibility of wireless sensors using ambient 2.4GHz RF energy," in *Proceedings of 2012 IEEE Sensors*, pp. 1–4, Oct. 2012.

[2] J. F. Ensworth and M. S. Reynolds, "BLE-backscatter: Ultra-low-power IoT nodes compatible with Bluetooth 4.0 Low Energy (BLE) smartphones and tablets." journal, submitted, revised, 2016.

[3] J. F. Ensworth and M. S. Reynolds, "Every smart phone is a backscatter reader: Modulated backscatter compatibility with Bluetooth 4.0 low energy (BLE) devices," in *2015 IEEE International Conference on RFID (IEEE RFID)*, April 2015.

[4] S. J. Thomas and M. S. Reynolds, "A 96 Mbit/sec, 15.5 pJ/bit 16-QAM modulator for UHF backscatter communication," in *2012 IEEE International Conference on RFID*, pp. 185–190, April 2012.

[5] S. J. Thomas, T. Deyle, R. Harrison, and M. S. Reynolds, "Rich-media tags: Battery-free wireless multichannel digital audio and image transmission with UHF RFID techniques," in *2013 IEEE International Conference on RFID*, pp. 231–236, April 2013.

[6] V. Pillai, H. Heinrich, D. Dieska, P. V. Nikitin, R. Martinez, and K. V. S. Rao, "An ultra-low-power long range battery/passive RFID tag for UHF and microwave bands with a current consumption of 700 nA at 1.5 v," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 54, pp. 1500–1512, July 2007.

[7] J. C. Jensen, R. Sadhwani, A. A. Kidwai, B. Jann, A. Oster, M. Sharkansky, I. Ben-bassat, O. Degani, S. Porat, A. Fridman, H. Shang, C. Chu, A. Ly, and M. Smith, "Single-chip WiFi b/g/n 1x2 SoC with fully integrated front-end & PMU in 90nm digital CMOS technologypmu in 90nm digital CMOS technology," in *2010 IEEE Radio Frequency Integrated Circuits Symposium*, pp. 447–450, May 2010.

[8] L. Nathawad, M. Zargari, H. Samavati, S. Mehta, A. Kheirkhahi, P. Chen, K. Gong, B. Vakili-Amini, J. Hwang, M. Chen, M. Terrovitis, B. Kaczynski, S. Limotyrakis, M. Mack, H. Gan, M. Lee, S. Abdollahi-Alibeik, B. Baytekin, K. Onodera, S. Mendis, A. Chang, S. Jen, D. Su, and B. Wooley, "A dual-band CMOS MIMO radio SoC for IEEE 802.11n wireless LAN," in *2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, pp. 358–619, Feb 2008.

[9] Y. H. Liu, C. Bachmann, X. Wang, Y. Zhang, A. Ba, B. Busze, M. Ding, P. Harpe, G. J. van Schaik, G. Selimis, H. Giesen, J. Gloudemans, A. Sbai, L. Huang, H. Kato, G. Dolmans, K. Philips, and H. de Groot, "A 3.7mW-RX 4.4mW-TX fully integrated Bluetooth Low-Energy/IEEE802.15.4/proprietary SoC with an ADPLL-based fast frequency offset compensation in 40nm CMOS," in *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, pp. 1–3, Feb 2015.

[10] W. Kluge, F. Poegel, H. Roller, M. Lange, T. Ferchland, L. Dathe, and D. Eggert, "A fully integrated 2.4-GHz IEEE 802.15.4-compliant transceiver for ZigBee trade; applications," *IEEE Journal of Solid-State Circuits*, vol. 41, pp. 2767–2775, Dec 2006.

[11] R. B. Staszewski, C.-M. Hung, K. Maggio, J. Wallberg, D. Leipold, and P. T. Balsara, "All-digital phase-domain TX frequency synthesizer for Bluetooth radios in 0.13 μm CMOS," in *2004 Digest of Technical Papers. ISSCC. 2004 IEEE International Solid-State Circuits Conference*, vol. 1, pp. 272–527, Feb 2004.

[12] B. W. Cook, A. Berny, A. Molnar, S. Lanzisera, and K. S. J. Pister, "Low-power 2.4-GHz transceiver with passive RX front-end and 400-mV supply," *IEEE Journal of Solid-State Circuits*, vol. 41, pp. 2757–2766, Dec 2006.

[13] "iPhone 6." 2016. [Online]. Available: http://www.apple.com/iphone-6/specs/.

[14] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, "Wi-Fi backscatter: Internet connectivity for RF-powered devices," in *Proceedings of ACM SIGCOMM*, August 2014.

[15] "Getting started with iBeacon." 2014. [Online]. Available: https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf, Dec 2014.

[16] N. Smith, "Pulsar P1 & P2 quartz wristwatch," *Engineering Technology*, vol. 8, pp. 101–102, December 2013.

[17] C. Narayanaswami, N. Kamijoh, M. Raghunath, T. Inoue, T. Cipolla, J. Sanford, E. Schlig, S. Venkiteswaran, D. Guniguntala, V. Kulkarni, and K. Yamazaki, "IBM's Linux watch, the challenge of miniaturization," *Computer*, vol. 35, pp. 33–41, Jan 2002.

[18] "fitbit surge." 2016. [Online]. Available: https://www.fitbit.com/surge, 2016.

[19] T. Monte, "Fitbit surge teardown." 2016. [Online]. Available: https://www.ifixit.com/Teardown/FitBit+ Surge+Teardown/42344, May 2016.

[20] J. F. Ensworth, S. J. Thomas, S. Y. Shin, and M. S. Reynolds, "Waveform-aware ambient RF energy harvesting," in *2014 IEEE International Conference on RFID (IEEE RFID)*, pp. 67–73, April 2014.

[21] K. Gudan, S. Chemishkian, J. J. Hull, S. J. Thomas, J. Ensworth, and M. S. Reynolds, "A 2.4 GHz ambient RF energy harvesting system with -20dBm minimum input power and NiMH battery storage," in *2014 IEEE RFID Technology and Applications Conference (RFID-TA)*, pp. 7–12, Sept 2014.

[22] K. Gudan, S. Shao, J. J. Hull, J. Ensworth, and M. S. Reynolds, "Ultra-low power 2.4GHz RF energy harvesting and storage system with -25 dBm sensitivity," in *2015 IEEE International Conference on RFID (RFID)*, pp. 40–46, April 2015.

[23] K. Gudan, S. Shao, J. J. Hull, A. Hoang, J. Ensworth, and M. S. Reynolds, "Ultra-low power autonomous 2.4GHz RF energy harvesting and storage system," in *2015 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, pp. 176–181, Sept 2015.

[24] J. F. Ensworth, A. T. Hoang, and M. S. Reynolds, "A timer based boost converter for RF energy harvesting," in *2015 IEEE Wireless Power Transfer Conference (WPTC)*, pp. 1–4, May 2015.

[25] J. F. Ensworth and M. S. Reynolds, "Devices and methods for backscatter communication using one of more communication protocols." Patent Application WO2016100887, Dec 2014.

[26] J. F. Ensworth, A. T. Hoang, T. Q. Phu, and M. S. Reynolds, "Full-duplex backscatter system using a Bluetooth Low Energy (BLE) receiver." to appear in Proceedings IEEE Radio Wireless Week 2017.

[27] J. F. Ensworth, A. T. Hoang, and M. S. Reynolds, "Ultra-low power wireless receiver for sensors and mobile devices." Patent Application.

[28] M. Mills, "Hearing aids and the history of electronics miniaturization," *IEEE Annals of the History of Computing*, vol. 33, pp. 24–45, Feb 2011.

[29] R. W. Evans, A. P. Ramsbottom, and D. W. Sheel, "Head-up displays in motor cars," in *Second International Conference on Holographic Systems, Components and Applications, 1989.*, pp. 56–62, Sep 1989.

[30] S. Thomas, J. Teizer, and M. Reynolds, "SmartHat: A battery-free worker safety device employing passive UHF RFID technology," in *2011 IEEE International Conference on RFID (RFID)*, pp. 85–90, April 2011.

[31] Y. T. Liao, H. Yao, A. Lingley, B. Parviz, and B. P. Otis, "A 3-uW CMOS glucose sensor for wireless contact-lens tear glucose monitoring," *IEEE Journal of Solid-State Circuits*, vol. 47, pp. 335–344, Jan 2012.

[32] H. Stockman, "Communication by means of reflected power," *Proceedings of the IRE*, vol. 36, pp. 1196–1204, Oct 1948.

[33] A. P. Sample, D. J. Yeager, P. S. Powledge, and J. R. Smith, "Design of a passively-powered, programmable sensing platform for UHF RFID systems," in *2007 IEEE International Conference on RFID*, pp. 149–156, March 2007.

[34] Y. Zhao and J. R. Smith, "A battery-free RFID-based indoor acoustic localization platform," in *2013 IEEE International Conference on RFID*, pp. 110–117, April 2013.

[35] S. Naderiparizi, A. N. Parks, Z. Kapetanovic, B. Ransford, and J. R. Smith, "WISPCam: a battery-free RFID camera," in *2015 IEEE International Conference on RFID (RFID)*, pp. 166–173, April 2015.

[36] D. Pharadia, K. R. Joshi, M. Kotaru, and S. Katti, "BackFi: High throughput WiFi backscatter," in *Proceedings of the 2015 ACM Conference on Special Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, 2015.

[37] J. D. Griffin and G. D. Durgin, "Multipath fading measurements at 5.8 GHz for backscatter tags with multiple antennas," *IEEE Transactions on Antennas and Propagation*, vol. 58, pp. 3693–3700, Nov 2010.

[38] X. Fu, A. Sharma, E. Kampianakis, A. Pedross-Engel, D. Arnitz, and M. S. Reynolds, "A low cost 10.0-11.1 GHz X-band microwave backscatter communication testbed with integrated planar wideband antennas," in *2016 IEEE International Conference on RFID (RFID)*, pp. 1–4, May 2016.

[39] C. Carlowitz, M. Vossiek, A. Strobel, and F. Ellinger, "Precise ranging and simultaneous high speed data transfer using mm-wave regenerative active backscatter tags," in *2013 IEEE International Conference on RFID (RFID)*, pp. 253–260, April 2013.

[40] J. Kimionis, A. Bletsas, and J. N. Sahalos, "Increased range bistatic scatter radio," *IEEE Transactions on Communications*, vol. 62, pp. 1091–1104, March 2014.

[41] J. Kimionis, A. Bletsas, and J. N. Sahalos, "Bistatic backscatter radio for power-limited sensor networks," in *2013 IEEE Global Communications Conference (GLOBECOM)*, pp. 353–358, Dec 2013.

[42] E. Kampianakis, J. Kimionis, K. Tountas, C. Konstantopoulos, E. Koutroulis, and A. Bletsas, "Wireless environmental sensor networking with analog scatter radio and timer principles," *IEEE Sensors Journal*, vol. 14, pp. 3365–3376, Oct 2014.

[43] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," in *SIGCOMM*, 2013.

[44] A. N. Parks, A. Liu, S. Gollakota, and J. R. Smith, "Turbocharging ambient backscatter communication," in *SIGCOMM*, 2014.

[45] Bletooth SIG, "Bluetooth specification version 4," tech. rep., The Bluetooth Special Interest Group, Kirkland, WA, USA, 2010.

[46] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith, "Passive Wi-Fi: Bringing low power to Wi-Fi transmissions," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, (Santa Clara, CA), pp. 151–164, USENIX Association, 2016.

[47] A. Sample and J. R. Smith, "Experimental results with two wireless power transfer systems," in *IEEE Radio and Wireless Symposium, 2009. RWS '09.*, pp. 16–18, Jan. 2009.

[48] S. Keyrouz, H. J. Visser, and A. G. Tijhuis, "Ambient RF energy harvesting from DTV stations," in *2012 Loughborough Antennas and Propagation Conference (LAPC)*, pp. 1–4, Nov. 2012.

[49] H. Nishimoto, Y. Kawahara, and T. Asami, "Prototype implementation of ambient RF energy harvesting wireless sensor networks," in *2010 IEEE Sensors*, pp. 1282–1287, Nov. 2010.

[50] S. Kitazawa, H. Ban, and K. Kobayashi, "Energy harvesting from ambient RF sources," in *2012 IEEE MTT-S International Microwave Workshop Series on Innovative Wireless Power Transmission: Technologies, Systems, and Applications (IMWS)*, pp. 39–42, May 2012.

[51] M. Arrawatia, M. S. Baghini, and G. Kumar, "RF energy harvesting system from cell towers in 900MHz band," in *2011 National Conference on Communications (NCC)*, pp. 1–5, Jan. 2011.

[52] U. Olgun, C.-C. Chen, and J. L. Volakis, "Efficient ambient WiFi energy harvesting technology and its applications," in *2012 IEEE Antennas and Propagation Society International Symposium (APSURSI)*, pp. 1–2, July 2012.

[53] H. Hong, X. Cai, X. Shi, and X. Zhu, "Demonstration of a highly efficient RF energy harvester for Wi-Fi signals," in *2012 International Conference on Microwave and Millimeter Wave Technology (ICMMT)*, vol. 5, pp. 1–4, May 2012.

[54] U. Olgun, C. C. Chen, and J. L. Volakis, "Design of an efficient ambient WiFi energy harvesting system," *Microwaves, Antennas Propagation, IET*, vol. 6, pp. 1200 –1206, 21 2012.

[55] U. Baroudi, A. Qureshi, S. Mekid, and A. Bouhraoua, "Radio frequency energy harvesting characterization: An experimental study," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1976 –1981, June 2012.

[56] H. J. Visser, A. C. F. Reniers, and J. A. C. Theeuwes, "Ambient RF energy scavenging: GSM and WLAN power density measurements," in *2008. EuMC 2008. 38th European Microwave Conference*, pp. 721 –724, Oct. 2008.

[57] W. C. Brown, "The technology and application of free-space power transmission by microwave beam," *Proceedings of the IEEE*, vol. 62, no. 1, pp. 11–25, 1974.

[58] A. N. Parks, A. P. Sample, Y. Zhao, and J. R. Smith, "A wireless sensing platform utilizing ambient RF energy," in *2013 IEEE Radio and Wireless Symposium (RWS)*, pp. 331–333, 2013.

[59] T. Ungan and L. M. Reindl, "Harvesting low ambient RF-sources for autonomous measurement systems," *2008. IEEE Instrumentation and Measurement Technology Conference Proceedings, 2008. IMTC* , pp. 62–65, May 2008.

[60] J. M. Damaschke, "Design of a low-input-voltage converter for thermoelectric generator," *IEEE Transactions on Industry Applications*, vol. 33, no. 5, pp. 1203–1207, 1997.

[61] S.-E. Adami, V. Marian, N. Degrenne, C. Vollaire, B. Allard, and F. Costa, "Self-powered ultra-low power DC-DC converter for RF energy harvesting," in *2012 IEEE Faible Tension Faible Consommation (FTFC)*, pp. 1–4, 2012.

[62] Y. K. Ramadass and A. P. Chandrakasan, "A battery-less thermoelectric energy harvesting interface circuit with 35 mV startup voltage," *IEEE Journal of Solid-State Circuits*, vol. 46, pp. 333–341, Jan. 2011.

[63] A. Richelli, S. Comensoli, and Z. M. Kovacs-Vajna, "A DC/DC boosting technique and power management for ultralow-voltage energy harvesting applications," *IEEE Transactions on Industrial Electronics*, vol. 59, pp. 2701–2708, June 2012.

[64] T. Sogorb, J. V. Llario, J. Pelegri, R. Lajara, and J. Alberola, "Studying the feasibility of energy harvesting from broadcast RF station for WSN," in *2008. IEEE Instrumentation and Measurement Technology Conference Proceedings, 2008. IMTC* , pp. 1360–1363, May 2008.

[65] R. J. Vyas, B. B. Cook, Y. Kawahara, and M. M. Tentzeris, "E-WEHP: A batteryless embedded sensor-platform wirelessly powered from ambient digital-TV signals," *IEEE Transactions on Microwave Theory and Techniques*, vol. 61, no. 6, pp. 2491–2505, 2013.

[66] W. Sanchez, C. Sodini, and J. L. Dawson, "An energy management IC for bioimplants using ultracapacitors for energy storage," in *2010 IEEE Symposium on VLSI Circuits (VLSIC)*, pp. 63–64, 2010.

[67] M. S. Trotter, J. D. Griffin, and G. D. Durgin, "Power-optimized waveforms for improving the range and reliability of RFID systems," in *2009 IEEE International Conference on RFID*, pp. 80–87, 2009.

[68] M. S. Trotter and G. D. Durgin, "Survey of range improvement of commercial RFID tags with power optimized waveforms," in *2010 IEEE International Conference on RFID*, pp. 195–202, 2010.

[69] C. R. Valenta and G. D. Durgin, "Rectenna performance under power-optimized waveform excitation," in *2013 IEEE International Conference on RFID (RFID)*, pp. 237–244, 2013.

[70] A. S. Boaventura and N. B. Carvalho, "Maximizing DC power in energy harvesting circuits using multisine excitation," in *2011 IEEE MTT-S International Microwave Symposium Digest (MTT)*, pp. 1–4, 2011.

[71] A. Collado and A. Georgiadis, "Improving wireless power transmission efficiency using chaotic waveforms," in *2012 IEEE MTT-S International Microwave Symposium Digest (MTT)*, pp. 1–3, 2012.

[72] A. Dolgov, R. Zane, and Z. Popovic, "Power management system for online low power RF energy harvesting optimization," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 7, pp. 1802–1811, 2010.

[73] C. M. Vigorito, D. Ganesan, and A. G. Barto, "Adaptive control of duty cycling in energy-harvesting wireless sensor networks," in *4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07.*, pp. 21–30, 2007.

[74] J. Colomer-Farrarons, P. Miribel-Catala, A. Saiz-Vela, and J. Samitier, "A multiharvested self-powered system in a low-voltage low-power technology," *IEEE Transactions on Industrial Electronics*, vol. 58, pp. 4250 –4263, Sept. 2011.

[75] H. Jabbar, Y. S. Song, and T. T. Jeong, "RF energy harvesting system and circuits for charging of mobile devices," *IEEE Transactions on Consumer Electronics*, vol. 56, pp. 247–253, February 2010.

[76] J. A. Paradiso and T. Starner, "Energy scavenging for mobile and wireless electronics," *IEEE Pervasive Computing*, vol. 4, pp. 18–27, Jan 2005.

[77] P. P. Mercier, A. C. Lysaght, S. Bandyopadhyay, A. P. Chandrakasan, and K. M. Stankovic, "Energy extraction from the biologic battery in the inner ear," *Nat Biotech*, vol. 30, pp. 1240–1243, 12 2012.

[78] Z. Zhu, T. Kin Tam, F. Sun, C. You, and Y. H. Percival Zhang, "A high-energy-density sugar biobattery based on a synthetic enzymatic pathway," *Nat Commun*, vol. 5, 01 2014.

[79] J. F. Ensworth, S. J. Thomas, S. Y. Shin, and M. S. Reynolds, "Waveform-aware ambient RF energy harvesting," in *2014 IEEE International Conference on RFID (IEEE RFID)*, pp. 67–73, April 2014.

[80] N. V. Desai, Y. K. Ramadass, and A. P. Chandrakasan, "A bipolar ±40 mV self-starting boost converter with transformer reuse for thermoelectric energy harvesting," in *International Symposium on Low Power Electronics and Design*, pp. 221–226, Aug 2014.

[81] P. Perez-Nicoli, P. Castro, and F. Silveira, "A series-parallel switched capacitor step-up DC-DC converter and its gate-control circuits for over the supply rail switches," in *2014 IEEE 5th Latin American Symposium on Circuits and Systems (LASCAS)*, pp. 1–4, Feb 2014.

[82] O. Lopez-Lapena, M. T. Penella, and M. Gasulla, "A closed-loop maximum power point tracker for subwatt photovoltaic panels," *IEEE Transactions on Industrial Electronics*, vol. 59, pp. 1588–1596, March 2012.

[83] S. J. Thomas, E. Wheeler, J. Teizer, and M. S. Reynolds, "Quadrature amplitude modulated backscatter in passive and semipassive UHF RFID systems," *IEEE Transactions on Microwave Theory and Techniques*, vol. 60, pp. 1175–1182, April 2012.

[84] Bluetooth SIG, Inc, "Bluetooth SIG 2014 Annual Report," 2015.

[85] B. Warneke, M. Last, B. Liebowitz, and K. S. J. Pister, "Smart dust: communicating with a cubic-millimeter computer," *Computer*, vol. 34, pp. 44–51, Jan 2001.

[86] M. Grover, S. K. Pardeshi, N. Singh, and S. Kumar, "Bluetooth low energy for industrial automation," in *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, pp. 512–515, Feb 2015.

[87] J.-R. Lin, T. Talty, and O. Tonguz, "On the potential of Bluetooth low energy technology for vehicular applications," *IEEE Communications Magazine*, vol. 53, pp. 267–275, January 2015.

[88] G. Rajagopal, V. Lodd, A. Vignesh, R. Rajesh, and V. Vijayaraghavan, "Low cost cloud based intelligent farm automation system using Bluetooth low energy," in *2014 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, pp. 127–132, Aug 2014.

[89] P. H. Chou, C.-T. Lee, Z.-Y. Peng, J.-P. Li, T. K. Lai, C.-M. Chang, C.-H. Yang, Y.-L. Chen, C.-C. Nien, L.-H. Chen, L.-Y. Lai, J.-C. Lu, and S.-C. Hung, "A Bluetooth-Smart insulating container for cold-chain logistics," in *2013 IEEE 6th International Conference on Service-Oriented Computing and Applications (SOCA)*, pp. 298–303, Dec 2013.

[90] M. Collotta and G. Pau, "A novel energy management approach for smart homes using Bluetooth low energy," *IEEE Journal on Selected Areas in Communications*, vol. 33, pp. 2988–2996, Dec. 2015.

[91] M. Ali, L. Albasha, and H. Al-Nashash, "A Bluetooth low energy implantable glucose monitoring system," in *2011 41st European Microwave Conference (EuMC)*, pp. 1265–1268, Oct 2011.

[92] Y.-J. Lin, H.-S. Chen, and M.-J. Su, "A cloud based Bluetooth low energy tracking system for dementia patients," in *2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*, pp. 88–89, Jan 2015.

[93] B. Yu, L. Xu, and Y. Li, "Bluetooth low energy (BLE) based mobile electrocardiogram monitoring system," in *2012 International Conference on Information and Automation (ICIA)*, pp. 763–767, June 2012.

[94] Y.-J. Park and H.-S. Cho, "Transmission of ECG data with the patch-type ECG sensor system using Bluetooth low energy," in *2013 International Conference on ICT Convergence (ICTC)*, pp. 289–294, Oct 2013.

[95] Z.-M. Lin, C.-H. Chang, N.-K. Chou, and Y.-H. Lin, "Bluetooth low energy (BLE) based blood pressure monitoring system," in *2014 International Conference on Intelligent Green Building and Smart Grid (IGBSG)*, pp. 1–4, April 2014.

[96] V. Talla, B. Kellogg, B. Ransford, S. Naderiparizi, S. Gollakota, and J. R. Smith, "Powering the next billion devices with Wi-Fi," in *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies*, no. 4 in CoNext '15, (New York, NY, USA), pp. 1–13, ACM, May 2015.

[97] V. Talla, S. Pellerano, H. Xu, A. Ravi, and Y. Palaskas, "Wi-Fi RF energy harvesting for battery-free wearable radio platforms," in *2015 IEEE International Conference on RFID (RFID)*, pp. 47–54, April 2015.

[98] Z. Popovic, S. Korhummel, S. Dunbar, R. Scheeler, A. Dolgov, R. Zane, E. Falkenstein, and J. Hagerty, "Scalable RF energy harvesting," *IEEE Transactions on Microwave Theory and Techniques*, vol. 62, pp. 1046–1056, April 2014.

[99] C. R. Valenta and G. D. Durgin, "Harvesting wireless power: Survey of energy-harvester conversion efficiency in far-field, wireless power transfer systems," *IEEE Microwave Magazine*, vol. 15, pp. 108–120, June 2014.

[100] J. D. Griffin and G. D. Durgin, "Complete link budgets for backscatter-radio and RFID systems," *IEEE Antennas and Propagation Magazine*, vol. 51, pp. 11–25, April 2009.

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

[102] P. V. Nikitin, K. V. S. Rao, and R. D. Martinez, "Differential RCS of RFID tag," *Electronic Letters*, vol. 43, pp. 431–432, April 2007.

[103] V. Iyer, V. Tall, B. Kellog, S. Gollakota, and J. R. Smith, "Inter-technology backscatter: Towards internet connectivity for implanted devices," *arXiv preprint arXiv:1607.04663*, 2016.

[104] P. V. Nikitin, S. Ramamurthy, R. Martinez, and K. V. S. Rao, "Passive tag-to-tag communication," in *2012 IEEE International Conference on RFID*, pp. 177–184, April 2012.

[105] S. J. Thomas, R. R. Harrison, A. Leonardo, and M. S. Reynolds, "A battery-free multi-channel digital neural/EMG telemetry system for flying insects," in *2011 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, pp. 229–232, Nov 2001.

[106] J. S. Besnoff, T. Deyle, R. R. Harrison, and M. S. Reynolds, "Battery-free multichannel digital ECG biotelemetry using UHF RFID techniques," in *2013 IEEE International Conference on RFID*, pp. 16–22, April 2013.

[107] "2.4 GHz Bluetooth Low Energy system-on-chip," tech. rep., Texas Instruments, October 2013.

[108] "nRF51822 Multiprotocol Bluetooth Low Energy/2.4 GHz RF System on a Chip," tech. rep., Nordic Semiconductor, 2014.

[109] "DA 14580 low power Bluetooth Smart SoC," tech. rep., Dialog Semiconductor, January 2015.

[110] "BLE112 data sheet," tech. rep., Bluegiga Technologies, 2011.

[111] NXP, "QN902x ultra low power Bluetooth LE system-on-chip solution," tech. rep., 2016.

[112] W. K. Kim, M. Q. Lee, J. H. Kim, H. S. Lim, J. W. Yu, B. J. Jang, and J. S. Park, "A passive circulator with high isolation using a directional coupler for RFID," in *2006 IEEE MTT-S International Microwave Symposium Digest*, pp. 1177–1180, June 2006.

[113] M. Koller and R. Küng, "Adaptive carrier supression for UHF RFID using digitally tunable capacitors," in *Microwave Conference (EuMC), 2013 European*, pp. 943–946, Oct 2013.

[114] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *ACM SIGCOMM*, 2013.

[115] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 1637–1652, Sept 2014.

[116] J. Zhou, T. H. Chuang, T. Dinc, and H. Krishnaswamy, "Integrated wideband self-interference cancellation in the RF domain for FDD and full-duplex wireless," *IEEE Journal of Solid-State Circuits*, vol. 50, pp. 3015–3031, Dec 2015.

[117] E. W. Herold and L. Malter, "Some aspects of radio reception at ultra-high frequencies: Part v. frequency mixing in diodes," *Proceedings of the IRE*, vol. 31, pp. 575–582, Oct 1943.

[118] M. R. Barber and R. M. Ryder, "Ultimate noise figure and conversion loss of the schottky barrier mixer diode," in *G-MTT International Symposium Digest*, vol. 66, pp. 13–18, May 1966.

[119] S. A. Maas, *The RF and Microwave Circuit Design Cookbook*. Artech House, 1998.

[120] D. K. Misra, *Radio-Frequency and Microwave Communication Circuits Analysis and Design*. John Wiley & Sons, Inc., 2004.

[121] Avago Technologies, "HSMS-286x series surface mount microwave schottky detector diodes," 2009.

[122] Avago Technologies, "Application note 1124: Linear models for diode surface mount packages," 2010.

[123] F. Hessar and S. Roy, "Energy based performance evaluation of passive EPC Gen 2 Class 1 RFID systems," *IEEE Transactions on Communications*, vol. 61, pp. 1337–1348, April 2013.

[124] I. i. Veen, Q. Liu, P. Pawelczak, A. Parks, and J. R. Smith, "BLISP: Enhancing backscatter radio with active radio for computational RFIDs," in *2016 IEEE International Conference on RFID (RFID)*, pp. 1–4, May 2016.

[125] D. Arnitz and M. S. Reynolds, "Multitransmitter wireless power transfer optimization for backscatter RFID transponders," *IEEE Antennas and Wireless Propagation Letters*, vol. 12, pp. 849–852, 2013.

[126] D. Arnitz and M. S. Reynolds, "Wireless power transfer optimization for nonlinear passive backscatter devices," in *2013 IEEE International Conference on RFID (RFID)*, pp. 245–252, April 2013.

[127] G. Lipworth, J. Ensworth, K. Seetharam, D. Huang, J. S. Lee, P. Schmalenberg, T. Nomura, M. S. Reynolds, D. R. Smith, and Y. Urzhumov, "Magnetic metamaterial super lens for increased range wireless power transfer," *Scientific Reports*, vol. 4, 2014.

[128] G. Lipworth, J. Ensworth, K. Seetharam, J. S. Lee, P. Schmalenberg, T. Nomura, M. S. Reynolds, D. R. Smith, and Y. Urzhumov, "Quasi-static magnetic field shielding using longitudinal mu-near-zero metamaterials," *Scientific Reports*, 2015.

Biography

Joshua Frederick Ensworth was born in Oswego, New York USA. He received the Bachelor of Science in Electrical Engineering (BSEE) and graduated manga cum laude from Tufts University in Medford, MA. Following two years working at Raytheon he enrolled at Duke University in 2011, and earned the Master of Science (MS) degree in 2014. Josh then received the Ph.D degree from the University of Washington in 2016, and his dissertation titled *Ultra-low-power BLE compatible communication and energy harvesting for battery-free wearable devices*, was written under the direction of Dr. Matthew S. Reynolds.

While working on his Ph.D degree, Josh was nominated for a best paper award and won a best poster/demo award at the 2015 IEEE RFID conference for his work *Every smart phone is a backscatter reader: Modulated backscatter compatibility with Bluetooth 4.0 low energy (BLE) devices.* At the time of publication of this dissertation, Josh has authored 2 published journal articles [127, 128] with another currently in review [2] and 7 peer-reviewed conference proceedings articles [79, 21, 3, 22, 24, 23, 26]. Josh has been a student member of the IEEE and Eta Kappa Nu since 2008.