Low Power Adaptive Wireless Circuits for the Internet of Things and In-body implants

by

Mohamed Radwan Abdelhamid

S.M., Massachusetts Institute of Technology (2017)
M.Sc, Electrical Engineering, Cairo University (2015)
B.Sc., Electrical Engineering, Cairo University (2013)

Submitted to the Department of Electrical Engineering and Computer Science

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2021

Author .....
Department of Electrical Engineering and Computer Science
May 19, 2021

Certified by .....
Anantha P. Chandrakasan
Vannevar Bush Professor of Electrical Engineering and Computer Science
Thesis Supervisor

Certified by .....
Fadel Adib
Doherty Associate Professor of the MIT Media Lab and EECS
Thesis Supervisor

Accepted by .....
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

Low Power Adaptive Wireless Circuits for the Internet of Things and In-body implants

by

Mohamed Radwan Abdelhamid

Submitted to the Department of Electrical Engineering and Computer Science
on May 19, 2021, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Electrical Engineering and Computer Science

Abstract

The emergence of the Internet of Things (IoT) and the desire for novel biomedical applications have resulted in growing demands for ultra low power wireless systems and circuits. To drive down energy consumption, conventional approaches for designing wireless systems focus on independently optimizing each of the layers of their designs: whether it is energy harvesting, sensor interface, security accelerators, or wireless protocols and MAC algorithms. While these approaches have delivered significant performance improvements, they remain inherently constrained by the performance of each respective layer.

This thesis demonstrates that by rethinking the abstractions across these layers and co-designing the entire stack of end-to-end wireless systems, we can build adaptive and ultra-low-power integrated systems with new capabilities and serve new applications. At the core of the innovations presented in this thesis are techniques that enable end-to-end adaptation ranging from reprogrammable antennas and harvesting circuits to adaptive wireless protocols and analog front-ends.

I demonstrate the value of my approach by designing, fabricating, and evaluating three end-to-end wireless systems each fully integrated in a 65nm CMOS IC for IoT and in-body applications. First, I present the first fully-integrated wireless and batteryless micro-implanted sensor which powers up by harvesting energy from RF signals and communicates at less than 400nW via backscatter. In contrast to prior designs which cannot operate across various in-body environments, my sensor can self-reconfigure to adapt to different tissues and channel conditions. Second, I present the first secure, wireless, and batteryless implantable sensor node for in-body pressure sensing. The node uses a piezoelectric sensor for in-body gastrointestinal (GI) pressure sensing and a loop antenna for wireless power and data communication. The pressure sensor front end, including the front-end amplifiers, achieves an efficiency of 4.3nJ/Conversion step with a resolution of 1.4mmHg. Third, I present a Bluetooth Low Energy wake-up receiver with a -80dBm sensitivity using a packet structure and a duty cycling scheme compliant with the Bluetooth Low Energy advertising protocol trading off power with latency. Event-driven applications achieve power lower than 240nW from a 0.75V

supply while latency-critical systems wake up in almost 200 microseconds. The thesis describes the design, implementation, and evaluation of each of these systems, and tests them in both simulation and representative real-world environments such as in-vitro and ex-vivo setups for biomedical implants.

Thesis Supervisor: Anantha P. Chandrakasan
Title: Vannevar Bush Professor of Electrical Engineering and Computer Science

Thesis Supervisor: Fadel Adib
Title: Doherty Associate Professor of the MIT Media Lab and EECS

Acknowledgments

These past six years wouldn't have been possible without the support and help of everyone around me and back home, each one is part of the reason I made it to the day I submit my thesis. Starting with my thesis advisor Prof. Anantha Chandrakasan who gave me the opportunity to join MIT and come to his group where there are the most brilliant circuit designers I've ever met. His guidance and support have been very important to my journey and personal development over the years. He managed to create this friendly and helpful work environment in the lab where you can easily just drop by other cubicles and start discussions or ask for help. I learned from Anantha how to be a mentor and how to tackle challenging circuit designs.

In the middle of my PhD journey, I started working with Prof. Fadel Adib as my thesis co-advisor and it has been a fun journey of excitement and full of thought-provoking discussions, brainstorming sessions, debugging, and the very frequent travels back and forth between EECS and the Media Lab. I learned from Fadel the importance of presenting my work to have the highest impact on the world and how hard work always pays off.

A special shoutout goes to my friends from Egypt: Karim, Kalabala, and the rest of the friends who always knew how to put a smile on my face despite the fact that we all live in different locations now. Also, my colleagues and friends in AnanthaGroup, especially Arun for all of his help in my BLE wake-up receiver chip and technical feedback preparing me for my first full tapeout. I have to mention Preet, Sirma, Vipasha, and Joanna for all the group lunches, late nights at the lab, and our midday procrastination circles. A special thank you goes to Utsav for being my cube neighbor for most of my PhD and his help in designing the security engine for my pressure sensing chip. Finally, I was lucky to be in two groups and I'm grateful for all my friends in the Signal Kinetics group with all of our meetings, virtual and non-virtual, and hikes. I'm grateful for Unsoo's help in my last chip both during design and testing. Ray and Joonhyuk have also been instrumental in the testing of my second chip.

I'd like to thank my Boston gang: Malik, Amira, Sally, Mahmoud, Aya, and

Mustafa for being part of my journey with our daily lunches, weekly outings, squash games, and getfit challenges. Moreover, I was fortunate to have a kind big brother, Mohammad Qasim, as my roommate for the past 5 years and who has been there with me through a lot: TQEs, RQEs, beach trips, Ramadans, and pandemic lockdown.

The last year wouldn't be possible without Salma Samir who brightens my days and always supports me in my lows and highs. She's always been there for me with unconditional love and support.

I have to thank my family for their unconditional love, my Mom and Dad for always cheering on me. My sisters, Reem and Salma, my brother Ahmed for all the happy memories and our gatherings in the Christmas breaks back home. And of course, my twin brother, Mostafa, who luckily ended up doing his PhD in the east coast and always flew to Boston on our birthdays. Lastly, my extended family here, my grandma, my aunt, my uncle, and cousins for all the fun and warmth at thanksgivings and long weekends.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

The growth and spread of the internet of things (IoT) networks demand the design of energy efficient nodes which are capable of communicating with the internet throughout different deployment conditions. With different estimates predicting more than 30 billion devices in 2025, IoT devices are expected to outnumber the human population with a ratio of almost 4 devices to 1 human [1].

In this thesis, I'm particularly interested in health applications and in-body implants. Over the past years, we witnessed the evolution of IoT devices for in-body sensing and health applications. It started with external sensors such as smart watches [2] and fitness trackers [3]; these are wearable devices which externally measure vital signs and transmit their data to the internet or to handheld devices. Advancing one step forward, IoT devices for in-body applications are moving inside the human body for sensing biomarkers from within. Starting with pacemakers to treat cardiac failures [4,5], the technological advances in both electronic design and biomedical sensor design are creating a network of devices in the ear canal with cochlear implants [6] and inside the colon through wireless endoscopy [7, 8].

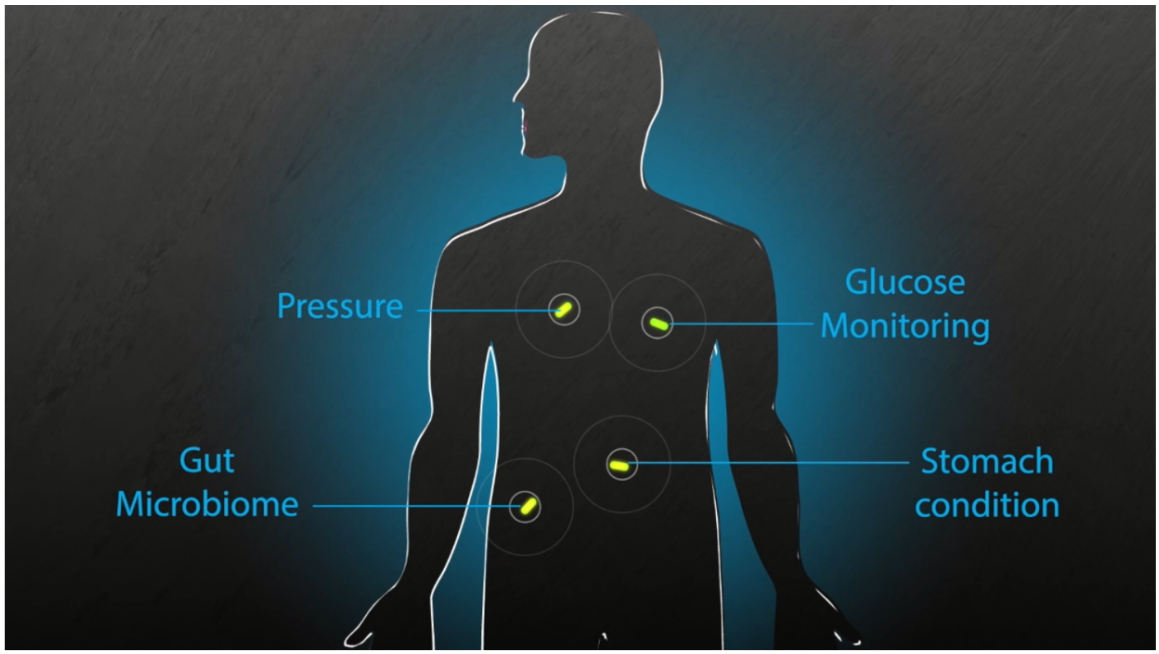


Figure 1-1: **In-body networks** In-body sensors work together to sense data from inside the human body and communicate them to the outside world.

While such devices pave the way for many applications in digital medicine where a patient would have a network of implants, as illustrated in Fig. 1-1, they still suffer from many limitations. These sensors can collect biodata such as internal pressure and temperature, gut microbiome conditions, or monitor the in-blood glucose level for diabetic patients but require a battery to be implanted deep inside the body which demands frequent invasive replacements. Batteryless operation through wireless charging serves as a potential candidate for these sensors providing wide applications ranging from artificial pancreas to deep brain stimulation, however, existing designs are still limited to shallow depths and have limited use-cases.

In its core, this thesis asks how to enable new applications for in-body implants allowing for wireless and batteryless deep-tissue operation. As illustrated in Fig. 1-2, I begin with the question of wirelessly powering up a batteryless implant in deep tissues. Then, I move to the challenge of ultra low power communication for battery-free sensor nodes. After enabling powering up and communication, I tackle the question of integrating sensing functionality with the wireless node. Once there is a stream

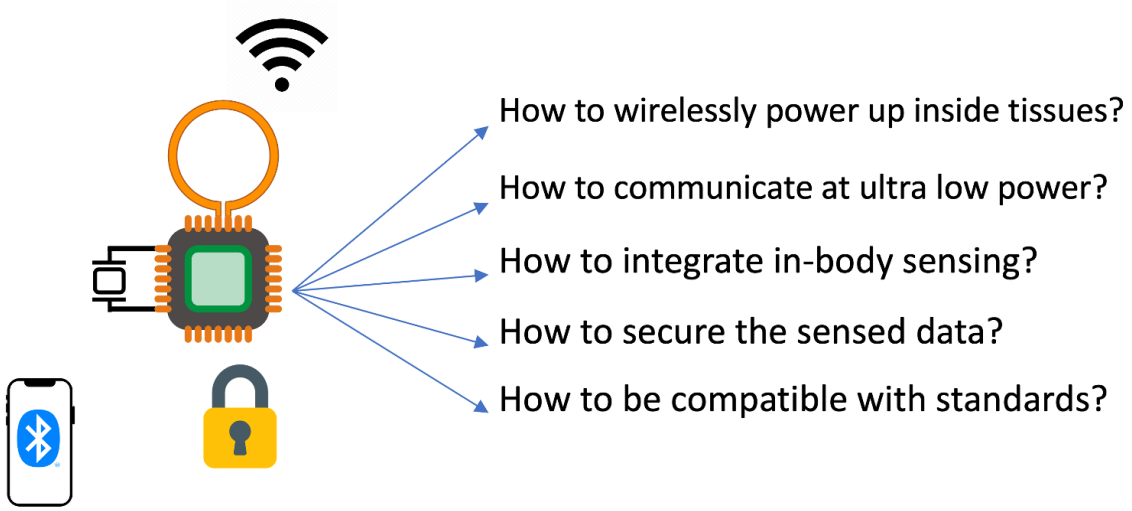


Figure 1-2: **Challenges for deep tissue implants** This thesis tackles the questions of powering up, communication, sensing, security, and standard compliance.

of sensed data, the question of securing the sensed data becomes a major concern. Finally, this thesis poses the question of compatibility with existing wireless standards and protocols such as Bluetooth-Low Energy.

1.2 Wireless Systems Built

This thesis tackles challenges in the low power wireless systems domain along three axes where a custom integrated circuit is designed and fabricated for each axis to provide a custom solution. Our contributions along these three directions are described in the following subsections.

1.2.1 μmedIC: the first wireless batteryless node for cross-tissue operation

We present the design, implementation, and evaluation of μmedIC, a fully-integrated wireless and batteryless micro-implanted sensor [9]. The sensor powers up by harvesting energy from RF signals and communicates at near-zero power via backscatter. In

contrast to prior designs which cannot operate across various in-body environments, our sensor can self-reconfigure to adapt to different tissues and channel conditions. This adaptation is made possible by two key innovations: an integrated hardware enabling a reprogrammable antenna that can tune its energy harvesting resonance to surrounding tissues, and a backscatter rate adaptation protocol that closes the feedback loop by tracking circuit-level sensor hints. We built our design on millimeter-sized integrated chips and flexible antenna substrates, and tested it in environments that span both in-vitro (fluids) and ex-vivo (tissues) conditions. Our evaluation demonstrates μmedIC's ability to tune its energy harvesting resonance by more than 200 MHz (i.e., adapt to different tissues) and to scale its bitrate by an order of magnitude up to 6Mbps, allowing it to support higher data rate applications (such as streaming low-res images) without sacrificing availability. This rate adaptation also allows μmedIC to scale its communication energy consumption by an order of magnitude down to 350 nanoWatts. These capabilities pave way for a new generation of networked micro-implants that can adapt to complex and time-varying in-body environments.

1.2.2 PZSense: the first wireless secure batteryless pressure sensor

We present the first secure, wireless, and batteryless implantable sensor node for in-body pressure sensing. The node integrates a piezoelectric sensor for in-body gastrointestinal (GI) pressure sensing and a loop antenna for wireless power and data communication with a 65nm CMOS IC. The system incorporates wireless energy harvesting, a low power analog front end with a fast-settling DC-cancellation loop, and achieves a pressure sensing resolution of 1.4mmHg with an efficiency of 4.3nJ/conversion step. Moreover, it employs a security engine for data encryption and transmitter authentication.

1.2.3 BLE WuRX: a -80dBm Bluetooth-Low Energy wake-up receiver with scalable power and latency

We present an FSK wake-up receiver with a -80 dBm sensitivity using a packet structure and a duty cycling scheme compliant with the Bluetooth-Low Energy (BLE) protocol trading off power with latency [10]. Event-driven applications consume power lower than 240nW from a 0.75V supply while latency-critical systems wake up in almost 200μs at a 230μW of active power consumption. A within-bit LC oscillator duty-cycling scheme is proposed to provide an extra 24% power reduction. Additionally, a custom FSK transmitter can trigger our wake-up receiver at 17nW only for an average latency of 5 seconds.

1.3 Thesis Outline

This thesis presents the designs of low power wireless systems with reconfigurable operation for different applications ranging from biomedical implants to IoT networks.

Chapter 2 provides a primer for wireless energy harvesting and backscatter communication links. Then, chapter 3 presents a platform for reconfigurable implantable nodes which can operate across different tissues through the use of programmable structures in the RF matching front-end, coupled microstrip antenna loading, and backscatter datarate. Then, it provides a detailed description of the wireless link, antenna design, and the circuits forming the different building blocks of the wireless batteryless in-body implant and concludes with the system evaluation.

Chapter 4 builds on the previous chapter to integrate a reconfigurable wireless front-end with a strain-based pressure sensor and a low power analog front end for biomedical data acquisition. It presents the proposed system architecture and illustrates the functionality through providing the test chip measurement results. Chapter 5 discusses the control logic which orchestrates the whole operation of the chip and explains

how the security engine utilizes Advanced Encryption Standard-Galois Counter Mode (AES-GCM) for data confidentiality and authenticity.

The third direction is outlined in chapter 6 which presents a duty-cycled BLE-compliant wake-up receiver for IoT networks. Then chapter 7 moves on to explore how to tackle the battery draining threats of replay attacks by adversary nodes in the network through the use of RF fingerprinting to perform transmitter classification using unique features in the transients of the RF BLE signal.

Finally, chapter 8 summarizes the thesis, draws conclusions, and outlines the lessons learned throughout these designs while providing a path for potential future directions.

Chapter 2

Background

Innovations in mm-sized implants are currently paving the road for revolutionary biomedical systems which will help us track diseases from deep inside the body and monitor them with handheld devices at the palm of our hand. Such advancements in implants design as well as signal processing will allow us to predict diseases based on the behavior of internal physiological function and even let us take the necessary measures to prevent such diseases from ever occurring.

The past two decades have witnessed an increased interest in bringing wireless capabilities to implantable devices. Research in the early 2000's focused on understanding the impact of RF signals on the human body [11, 12], and was propelled by the rise of body area networks [13]. The success of this research and technological agenda resulted in wide adoption of wireless communication in implantable medical devices such as implanted pacemakers, cardiac defibrillators, insulin pumps, and capsule endoscopes [14, 15]. These early systems were all battery-powered [13].

The success of this body of work has prompted researchers to extend the vision beyond wireless communication to in-body wireless power transfer [16, 17]. Power transfer can eliminate the need for batteries which would, in turn, allow implantable sensors to function longer (without surgical replacement) and can result in a significant

reduction in their form factor (since batteries can occupy 50% or more of the sensor's size [8]). These capabilities can significantly expand the potential use cases of in-body sensors to tumor monitoring, neural stimulation, and drug delivery [18–21]. The promise of such sensors has prompted the US Office of Science and Technology to declare long-lasting wireless micro-implants as one of six grand challenges of the decade [22].

2.1 Signal Propagation

In body communication entails a complex channel propagation model in which the transmitted signal gets reflected as well as refracted through the multiple body layers starting from skin towards muscles, fats, tissues and bones. The electromagnetic propagation throughout each individual layer of the body is governed by the relative dielectric permittivity of each medium (ϵ_r). In general, the permittivity is a frequency dependent complex quantity which defines the medium losses as well as the signal propagation velocity. Experimental data of electric permittivity of different body tissues is populated in [23] from as low as 10Hz of frequency up to 100GHz.

Several empirical parametric models have been introduced in the literature over the past two decades to characterize the frequency dependence of such complex permittivity, and hence, predict the properties of electromagnetic waves propagating through such media incurring all sorts of reflection, refraction and losses. One well-known model is the multiple Cole-Cole dispersion model [23] which parameterizes the permittivity at different frequncy regions such that:

$$\epsilon(\omega) = \epsilon_\infty + \sum_n \frac{\Delta\epsilon_n}{1 + (j\omega\tau_n)^{(1-\alpha_n)}} + \frac{\sigma}{j\omega\epsilon_0} \tag{2.1}$$

$$= \epsilon' - j\epsilon'' \tag{2.2}$$

where $\Delta\epsilon_n$, τ_n, and α_n are empirical parameters for fitting the permittivity along

different regions of frequency ω. Additionally, σ is the medium conductivity and ϵ_∞ is the infinite frequency dielectric constant while ϵ' and ϵ'' denote the real and imaginary components of the permittivity.

An electromagnetic signal propagating along these tissues experiences a path loss which is characterized by the propagation factor γ given by:

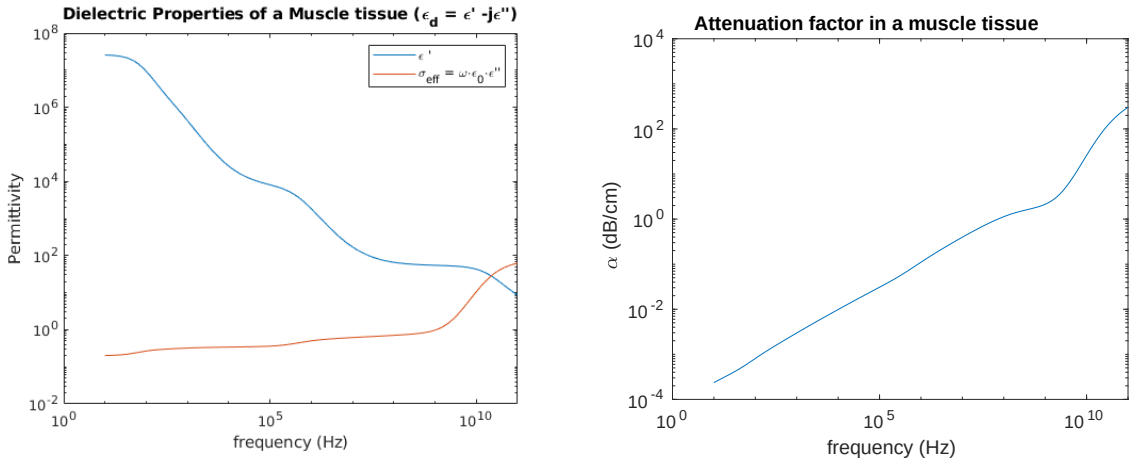
$$\gamma = j\omega\sqrt{\mu\epsilon} = \alpha + j\beta \tag{2.3}$$

where μ is the magnetic permeability of the tissue, which can be approximated to be that of air, α is the attenuation loss, and β is the propagation constant.

For instance, the dielectric properties of a muscle tissue is shown in Fig. 2-1 where it has a dielectric constant of $\epsilon_m = 55 - 17.4j$ and an attenuation factor of about $\alpha_{dB} \approx 2dB/cm$ at a frequency of 1 GHz around the biomedical ISM bands of interest.

With a frequency varying response, selecting the center frequency of operation becomes a matter of balancing out the system trade-offs. For instance, on one side, operating at a higher frequency in the mm-wave range allows for a graceful implant miniaturization where the antenna can be designed in a sub-mm size with good efficiency. However, the main drawback here for in-body communication is the fact that the attenuation factor grows exponentially and even superexponentially at certain bands with frequency.

A commonly used sweet spot for in-body communication networks is around the 1 GHz frequency where the tissue losses can be only around 1-4 dB/cm while the antenna size, which is typically designed to be an electrically small inductive antenna, can still be designed in the sub-cm or even the mm-size domain. One other factor which aids the smaller antenna size is that the velocity of the electromagnetic wave inside the tissues decreases due to the higher electric permittivity of the human tissues where $v = \frac{C}{\sqrt{\epsilon_r}}$ and C is the speed of light in vacuum, hence, the effective wavelength



a) Permittivity and conductivity

b) Attenuation factor

Figure 2-1: **Dielectric properties of a muscle tissue.** The figure uses the Cole-Cole model of a muscle tissue to plot (a) the real permittivity and the effective conductance, and (b) the attenuation factor as functions of frequency.

$\lambda_{eff} = \frac{v}{f}$ gets shorter allowing for smaller-sized in-body antennas.

2.2 Harvesting efficiency vs backscattering throughput

In order to analyze the different trade-offs of a batteryless passive backscattering implant. We begin by analyzing the power received by an RFID tag at a wavelength λ and a distance R from the reader. Such link is governed by Friis equation [24] such that:

$$P_{tag} = P_{TX} G_{TX} \left(\frac{\lambda}{2\pi R}\right)^2 G_{RX}(1 - |\Gamma_{RX}|^2) \tag{2.4}$$

where P_{TX} is the transmitted power, G_{TX} and G_{RX} are the transmitter and receiver antenna gains respectively, Γ_{RX} is the reflection coefficient at the receiver side which, for a complex load, is given by:

$$\Gamma_{RX} = \frac{Z_{rect} - Z_A^*}{Z_{rect} + Z_A} \tag{2.5}$$

where Z_A is the antenna's input impedance while Z_{rect} is the input impedance of the rectifier.

In a rectenna where the rectifier is perfectly resonated with the antenna, i.e. conjugately matched, such power produces a passively amplified voltage across the rectifier terminals:

$$\begin{aligned} V_{in}^2 &= 8\eta_A R_A Q_{eff}^2 P_{tag} && (2.6) \\ &= 8P_{TX}G_{TX}\Big(\frac{\lambda}{2\pi R}\Big)^2 G_{RX}(1-|\Gamma_{RX}|^2)\eta_A Q_{eff}^2 && (2.7) \end{aligned}$$

where η_A and R_A are the antenna efficiency and resistance respectively while Q_{eff} is the effective quality factor of the rectenna system. Then an N-stage non-linear rectifier produces a DC voltage of

$$V_{DC} = N(V_{in} - V_D) \tag{2.8}$$

where N is the number of stages and V_D is the drop voltage across the rectifying device when it turns on. For a resistive load or a constant current, this delivers an output power of

$$P_L = \frac{V_{DC}^2}{R_L} = V_{DC} I_L \tag{2.9}$$

Therefore, the energy harvesting efficiency can be defined as

$$\eta_{EH} = \frac{P_L}{P_{TX}} \propto G_{TX}G_{RX}(1-|\Gamma_{RX}|^2)Q_{eff}^2 \tag{2.10}$$

This shows that the energy harvesting efficiency depends quadratically on the system quality factor, the matching, as well as the antenna gains.

On the other hand, the uplink communication link budget can be derived by applying Friis equation twice, once from the reader to the tag which represents the powering up signal, then a second time when the signal backscatters and travels the

same distance back to the reader.

$$P_{reader} = P_{TX} G_{TX}^2 G_{RX}^2 \Big(\frac{\lambda}{2\pi R}\Big)^4 M \tag{2.11}$$

where M is the amplitude modulation factor defined by the average difference in reflection between the two different transmission states $M = \frac{1}{4}|\Gamma_1 - \Gamma_0|^2$.

Therefore, the signal to noise ratio (SNR) at the reader side is given by:

$$SNR_{reader} = \frac{P_{reader}}{N_{reader}} \propto G_{TX}^2 G_{RX}^2 M \tag{2.12}$$

Comparing equations (2.10) and (2.12), we clearly see that the communication link depends only on the antenna gains as well as the modulation factor of the tag while the energy harvesting efficiency is tied to the high quality factor value of the rectenna system.

Building upon this, we realize that for a high throughput deep tissue in-body network, the modulation factor M needs to be high over a wide band of frequencies in order to allow for high rates of communication at an adequate SNR. However, there is a direct trade-off between matching and bandwidth set by the Bode-Fano criterion limit [25]:

$$\int_0^\infty \ln\left(\frac{1}{|\Gamma(\omega)|}\right) d\omega \leq \frac{\pi\omega_0}{Q_L} \tag{2.13}$$

where $\Gamma(\omega)$ is the reflection coefficient as a function of frequency, ω_0 is the center frequency, and Q_L is the load's quality factor at the center frequency. To further understand such limit, let's consider a piecewise brickwall approximation of the reflection coefficient as:

$$\Gamma(\omega) = \begin{cases} \Gamma_{min} & \text{in the passband: } \omega_0 - \frac{\Delta\omega}{2} < \omega < \omega_0 + \frac{\Delta\omega}{2} \\ 1 & \text{in the stopband: otherwise} \end{cases} \tag{2.14}$$

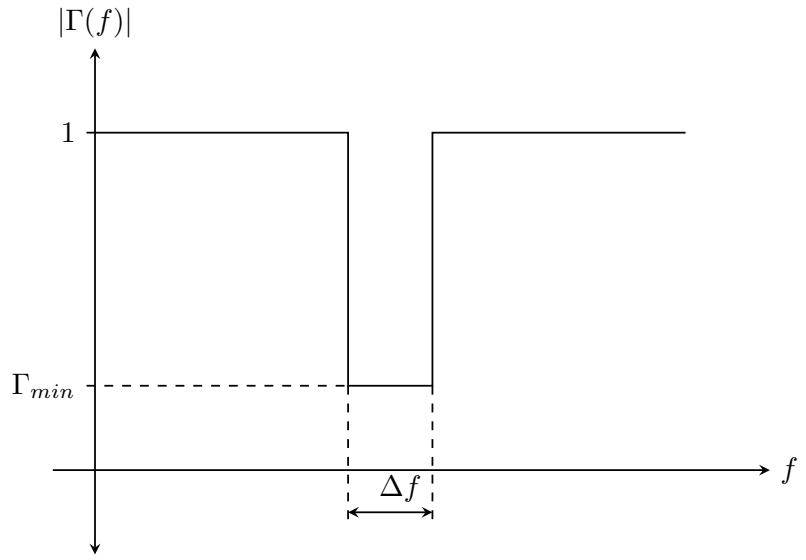


Figure 2-2: **Bode Fano Limit.** A brick wall approximation of the reflection coefficient illustrates the direct trade-off between matching and BW.

where Γ_{min} is the minimum reflection coefficient across the frequency bands as illustrated in Fig. 2-2.

Then, the Bode-Fano limit simplifies to:

$$\Delta\omega \cdot \ln\left(\frac{1}{|\Gamma_{min}|}\right) \leq \frac{\pi\omega_0}{Q_0} \tag{2.15}$$

$$B_\infty = \frac{\pi}{Q_L \cdot \ln\left(\frac{1}{|\Gamma_{min}|}\right)} \tag{2.16}$$

where B_∞ is the fractional bandwidth in the brickwall approximation, i.e. with an infinite combinations of LC matching elements. This shows that the bandwidth is inversely proportional to the best matching achieved across the band of interest. As real systems, such as second order LC tanks, have non-zero out of band absorption, the bandwidth is even lower than the Brickwall approximation ($B_{n^{th}-order} < B_\infty$). However, as the order increases, the bandwidth approaches the Bode-Fano limit.

Therefore, we need to provide a smart system which scales from one end of the spectrum to the other. Initially, it could start in a high-Q, high efficiency state such that it maximizes its probability to power up under the worst channel conditions.

Once it has enough power to turn on, it would be able to trade-off its high efficiency for a wider bandwidth through a reconfigurable coupled structure allowing for throughput enhancements up to an order of magnitude in the best case scenario.

2.3 Rectenna Optimization

To achieve the highest energy harvesting efficiency, the antenna and the rectifier have to be co-optimized in a *rectenna* design process as outlined in [26]. The antenna is designed as an electrically small inductive microstrip antenna whose impedance is given by an imaginary inductive component defined by L_A, and a real resistive part defined by the radiation resistance R_{rad} in addition to the conductive losses R_{loss}:

$$L_A = \mu R \left(\ln \left(\frac{8w}{R} \right) - 2 \right) \tag{2.17}$$

$$R_{rad} = 31171 \left(\frac{\pi R^2}{\lambda^2} \right)^2 \tag{2.18}$$

$$R_{loss} = \frac{R}{w} \sqrt{\frac{2\pi f \mu}{\sigma}} \tag{2.19}$$

where R is the antenna radius, w is its trace width, λ is the wavelength, f is the frequency, μ is the permeability, and σ is the conductivity.

Similarly, analyzing an N-stage rectifier yields a steady state input impedance given by:

$$R_{rect} = \frac{R_{1stg}}{N} \tag{2.20}$$

$$C_{rect} = NC_{1stg} + C_p \tag{2.21}$$

where R_{1stg} is the single stage resistance, C_{1stg} is the single stage capacitance, and C_p is the associated routing and packaging parasitic capacitance.

The number of stages (N), the width of the rectifying transistors, and the di-

mensions of the antenna are optimized to achieve the optimum sensitivity given the matching and quality factor constraints defined in equations (2.7)–(2.10).

As the optimization problem has many variables, an iterative approach of simulations is followed including both the rectifier parameters as well as the antenna variables to converge to the most optimum design.

Chapter 3

Self-Reconfigurable in-body implants

3.1 Introduction

The mobile networking community has recently witnessed mounting interest in wireless and batteryless sensors that can operate inside the human body [18, 19, 21, 27]. These sensors can power up by harvesting energy from RF (Radio Frequency) signals transmitted from outside the body, and they communicate at near-zero power via backscatter – i.e., by reflecting existing signals rather than transmitting their own carrier. The combination of energy harvesting and backscatter communication allows these sensors to be batteryless. Independence of batteries eliminates the need for surgical replacement, allows ultra-long term operation, and enables miniature, fully-integrated form factors [28]. As a result, such sensors could be used for continuous monitoring of biomarkers and tumors, ultra-long lasting drug delivery systems (e.g., for patients with Alzheimer's or Osteoporosis), and closed-loop control systems with real-time feedback (e.g., artificial pancreas for Diabetes' patients).

A key challenge that faces existing solutions for wireless and batteryless micro-implants lies in their rigid designs which cannot adapt to different tissues or to time-varying in-body conditions. This is particularly problematic for mobile sensors

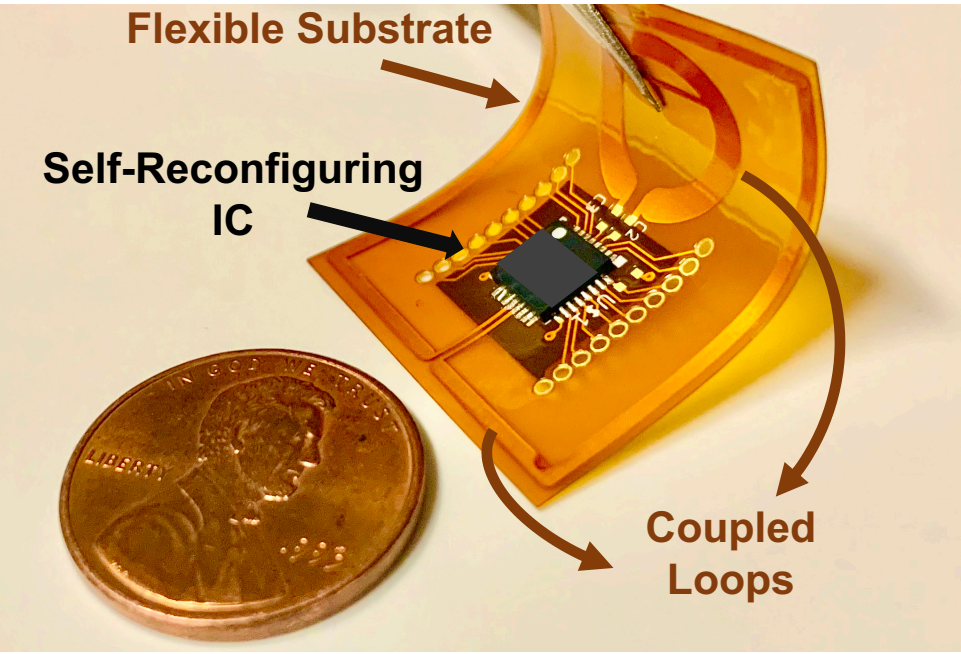


Figure 3-1: **μmedIC.** The self-reconfiguring hardware is implemented on an IC that controls the bi-resonance design on a flexible substrate. The penny is shown next to the micro-implant to demonstrate the form factor. μmedIC's flexible, thin design allows folding into an ingestible capsule or laminating it on an organ.

like ingestible capsules, which experience a variety of in-body environments as they travel through the digestive tract to deliver drugs or sense biomarkers. The ability to adapt to different in-body environments is also key to enabling these sensors to operate across different humans, whose bodies have different tissue compositions (fat, muscles, etc.). The majority of existing solutions side-step this challenge by limiting themselves to shallow depths (i.e., on the body or right under the skin) [18, 27, 29], where the ability to harvest energy is less impacted by the surrounding environment. Recent proposals (like IVN and ReMix) have tried to operate at larger depths at the expense of isolating the sensor (e.g., placing it in a test tube surrounded by air before implanting it inside tissues) [21] or by giving up energy harvesting altogether [19]. Additionally, these works have focused on optimizing the energy harvesting efficiency which limits their datarates to less than 1Mbps due to the trade-off between high efficiency and bandwidth.

We present μmedIC, a fully-integrated wireless and batteryless sensor that can adapt to varying in-body conditions and can be directly integrated with tissues. Similar to past proposals, μmedIC harvests energy from RF signals to power up and adopts backscatter to enable energy-efficient communication. In contrast to past proposals, μmedIC introduces multiple innovations that allow it to adapt its energy harvesting to surrounding tissues and its communication throughput to in-body conditions. Moreover, μmedIC's design is implemented on an IC and flexible antenna substrate; this design allows rolling it into the form of an ingestible capsule or laminating it on tissues (e.g., on the stomach wall), enabling intimate integration with the human body.

Before we describe how μmedIC operates, let us understand why it is difficult for batteryless in-body sensors to operate across different in-body environments. Consider a sensor that needs to power up and communicate in the 900 MHz ISM band, which is known to be optimal for energy-harvesting micro-implants [30].[1] In order to optimize energy harvesting, micro-implants are typically designed to resonate around the desired frequency of operation. The resonance frequency is determined by the shape of the antenna as well as the surrounding tissues (specifically, the dielectric of tissues in its immediate vicinity) [31]. Unfortunately, due to dependence on surrounding tissues, if a micro-implant is designed to resonate at 900 MHz in a certain tissue (e.g., muscle), its resonance shifts to a different frequency (e.g., 1.1 GHz) when placed in another tissue (e.g., fat). Fig. 3-2 shows this problem by plotting the harvested voltage as a function of frequency for fat (red plot) and muscle (blue plot), which exhibit different resonance frequencies (peaks) due to their different properties as previously discussed in section 2.1. This makes it infeasible to design batteryless micro-implants that can harvest energy across different tissues or maintain reliable backscatter communication if they need to travel through the human body. Furthermore, transmitting at frequencies

[1] In contrast, the MICS band around 400MHz is used for larger battery-powered implants such as cardiac pacemakers.

outside the ISM band (e.g., around 1.1 GHz) to power up the sensor would make the system incompliant with FCC regulations for consumer electronics.

At the heart of μmedIC's approach is a programmable "coupled" antenna design. Antenna coupling is a well-known phenomenon and refers to the interaction between two antennas when they are close to each other. Because coupling alters the antenna resonance, it is generally considered harmful [32], and communication engineers typically try to separate antennas from each other to minimize coupling. In contrast, μmedIC employs coupling in order to control the resonance and adapt it to surrounding tissues. The design consists of two antenna loops (as shown in Fig. 3-1): an inner circular loop and outer rectangular loop. Because the two loops are in close proximity, they "couple" with each other, resulting in a resonance frequency that depends on both. μmedIC can reprogram this resonance by tuning a capacitive load on both the outer loop and the inner loop. For example, it can leverage this property to reprogram the resonance in muscle back to the 900 MHz band as depicted by the green plot in Fig. 3-2. In section 3.4, we describe this approach in detail, the rationale for antenna design, as well as how μmedIC's bi-loop design allows it to reprogram both the antenna and the matching hardware.

So far, we have assumed that μmedIC knows its surrounding environment (i.e., tissue composition and channel conditions) and can choose the best configuration to match that environment. However, in practice, such information is not available and difficult to predict. To deal with this uncertainty, μmedIC exploits circuit-level hints to perform rate and resonance adaptation. At a high level, it senses the harvested energy (voltage) and uses it for rate adaptation. μmedIC conservatively starts with a high-efficiency configuration and gradually increases its throughput. In section 3.5, we describe this protocol in detail and show how μmedIC leverages low-level sensor hints to close the loop on rate adaptation.

We built a prototype of our design by fabricating it on an IC (shown in Fig. 3-1)

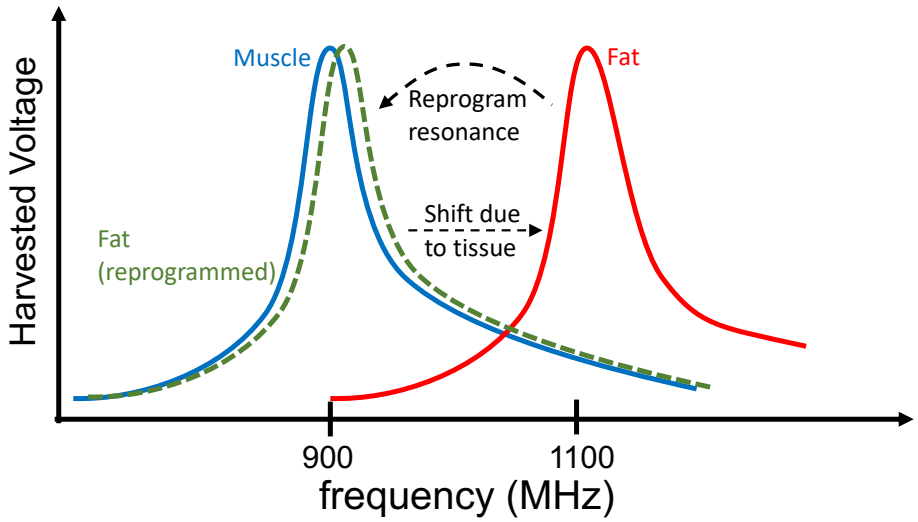


Figure 3-2: **Reprogramming Resonance.** The figure plots the harvested voltage versus frequency for a micro-implant placed in fat (red) and muscle (blue), demonstrating a shift in the resonance frequency. By reprogramming its resonance, μmedIC can move the resonance frequency back to 900 MHz allowing efficient harvesting and communication.

and integrating it with a re-programmable antenna on a flexible substrate. The design also integrates a MAC protocol that allows it to scale to multiple sensors. Our evaluation in both in-vitro (fluids) and ex-vivo (tissues) conditions demonstrates the following results:

- μmedIC's programmable resonance allows it to harvest energy across different types of tissues including fat, muscle, and multi-layer compositions with muscle, fat, and bones as well as different fluids. The resonance can be reconfigured by as much as 200 MHz inside tissues. In the absence of reconfigurability, the micro-implant's ability to power up reduces to one or two tissues.

- μmedIC can support bitrates reliably up to 6 Mbps and as low as 625 kbps. Its rate adaptation can gracefully scale to different in-body conditions by incorporating feedback through sensor hints. In the absence of rate adaptation, the design becomes either limited to low availability or low throughput.

Contributions. We present the first batteryless micro-implanted system that is capable of self-reconfiguration for energy harvesting and backscatter communication inside tissues. The system introduces a reconfigurable architecture with programmable antennas, harvesting circuits, and backscatter throughput. The design also introduces a rate and resonance adaptation protocol for wireless micro-implants. We also present a prototype implementation on an integrated circuit on a flexible antenna substrate and evaluation in different tissues.

We note that μmedIC's benefits extend beyond micro-implants that are entirely batteryless. For example, in higher data-rate applications (such as streaming images from endoscope capsules), today about half the energy is spent on RF transmissions [15, 19]. By enabling efficient and reconfigurable backscatter, μmedIC can significantly reduce the power consumption of such implants, allowing for battery-assisted implementations [33] that can function longer. As the technology evolves, it may also be integrated with recent proposals on battery-free cameras (which have been demonstrated outside the human body) [34]. Such designs are beyond the scope of this chapter and are left for future work.

3.2 Related Work

(a) Antenna Reconfigurability. Antenna reconfigurability can refer to a variety of techniques such as beamforming [35], polarization change [36], and frequency tuning [37]. μmedIC's design is most related to past work on frequency reconfiguration that aims to reuse the same antenna front-end for different frequency bands (e.g., LTE vs 5G). Operating inside the body, however, introduces at least two new unique challenges: first, in contrast to air – which is a homogeneous medium from an RF perspective – the human body is neither homogeneous nor predictable as it consists of different layers of tissues which vary across individuals and across body parts.

Second, μmedIC's design not only needs to shift the antenna itself, but also the entire resonant structure (i.e., antenna+rectifier); which introduces additional complexity to the reconfiguration problem if one wishes to maintain high efficiency as we explained in section 3.4.[2] μmedIC's architecture allows it to overcome these challenges while maintaining a near-zero power budget and operating inside tissues.

One of the major challenges that still faces in-body wireless applications is the low efficiency of implantable antennas [12, 39]. This low efficiency (around 1%) has been widely documented in literature on wireless communication with battery-powered medical implants [31, 40], and it becomes even more problematic for batteryless micro-implants that rely on harvested RF energy to power up [19, 21]. Recent advances in energy harvesting try to address this problem by resorting to *resonant* rectennas, where the antenna and the rectifier (energy harvester) are designed to resonate in order to maximize their harvesting efficiency [41, 42]. Such resonance, however, is significantly impacted by surrounding tissues; prior work has demonstrated that if tissue composition or depth changes, antennas can easily shift out of resonance, becoming inefficient [43, 44]. This is why the majority of existing in-body sensors still require batteries or remain limited to shallow depths where they can harvest enough energy to power up despite their low efficiency [19, 29]. Our work is motivated by this past literature on resonant rectennas and extends it to work across tissues by introducing reconfigurability to the design of wireless and batteryless micro-implants.

(b) Deep-Tissue RF. μmedIC's design also builds on recent work on in-body RF backscatter. Recent designs have demonstrated RF backscatter in shallow tissues [18, 27] as well as the potential of operating deeper inside the body [19, 21]. Such designs, however need to isolate the antenna from nearby tissues by isolating the implant inside a test-tube or by forgoing energy harvesting [19, 21]. Prior work has also explored mechanisms to improve signal-to-noise ratio (SNR) of in-body backscatter [45] but

[2]Specifically, in-air antennas can assume 50 Ohm matching, which would not be desirable for high harvesting efficiency [38].

also ignored the impact of surrounding tissues, which resulted in non-FCC compliant behavior. Our work directly advances this line of work and introduces resonance reconfigurability to enable embedding batteryless backscatter micro-implants directly in tissues.

(c) Backscatter Communication. Furthermore, μmedIC builds on a large and growing literature in backscattering different technologies, such as WiFi, TV signals, and Bluetooth [18,46–48]. Our contributions are orthogonal and can be combined with these past proposals if one wishes to operate the micro-implants at their other frequency bands (albeit operating at higher frequencies would introduce more attenuation [30]). Prior work has also explored bitrate adaptation for backscatter, primarily in the context of RFIDs [49, 50], but also for ambient backscatter [51]. μmedIC's rate adaptation is similarly motivated by the desire to reduce overhead, and it enables more efficient rate adaptation by tracking sensor hints in the IC itself.

(d) Non-RF In-Body Wireless. μmedIC is related to a large body of literature on in-body powering and communication using other approaches such as ultrasound [52], near-field [53], midfield [54], and capacitive coupling [55]. These approaches require either direct or near-direct contact with the body, and, as a result, have different application domains than RF-based systems like ours which can operate from larger distances outside the body [21, 27]. Thus, longer-range RF-based systems like μmedIC would result in more user-friendly implementations and pave way for easier remote and/or mobile healthcare solutions.

3.3 System Overview

μmedIC is a fully-integrated wireless and batteryless sensor for micro-implants that operate in the UHF (Ultra-High Frequency) ISM Band (902-928 MHz). The sensor can be used to support a variety of in-body monitoring and sensing applications such

as tracking biomarkers or long-term monitoring of internal vitals to allow for early intervention.

A μmedIC sensor powers up by harvesting energy from RF signals transmitted by a reader outside the body. The sensor decodes the reader's downlink commands and transmits its own packets on the uplink to be decoded by the reader. The design extends to multiple sensors, each of which is uniquely addressable. In the presence of multiple sensors, the reader orchestrates medium access.

The overall architecture of a μmedIC sensor is shown in Fig. 3-3. The design consists of a system-on-chip (SoC) that supports energy harvesting, decoding, and backscatter communication. μmedIC's SoC also incorporates a power management unit to support the various computing and communication tasks and an extensible interface that allows integrating the chip with external sensors. The 1 mm^2 chip is assembled on a flexible PCB with a custom printed antenna.

μmedIC can self-reconfigure to adapt to different in-body environments. There are two key components of this self-reconfiguration: the first is a reprogrammable bi-loop antenna that can adapt to surrounding tissues (section 3.4) and the second is a rate adaptation algorithm that tracks circuit-level sensor hints and adapts to channel conditions (section 3.5). The antenna and rate reprogrammability can be orchestrated by the IC itself. The next sections describe these components in detail.

3.4 Reprogrammable In-Body Rectenna

In this section, we describe the design of μmedIC's reprogrammable rectenna and demonstrate how this design enables adapting to different tissues in order to ensure efficient energy harvesting across various in-body environments.

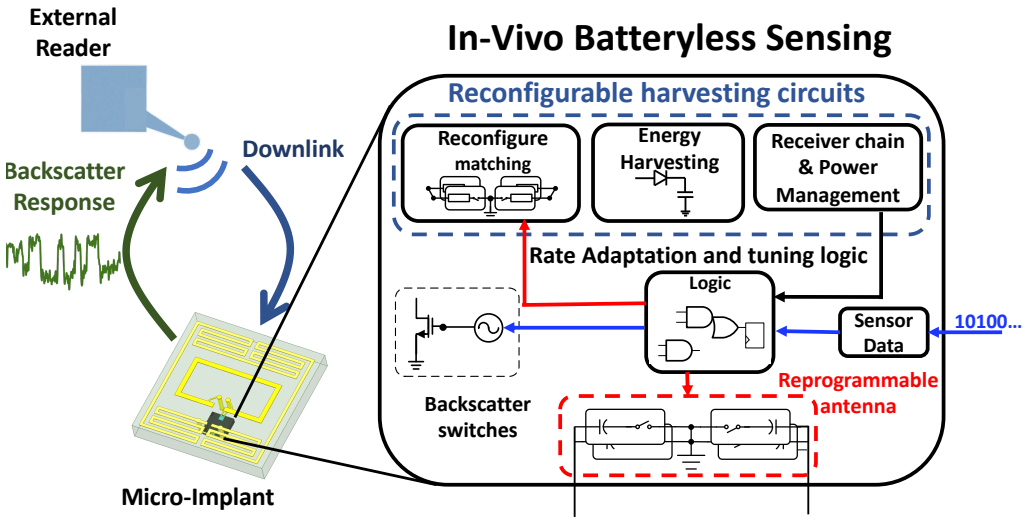


Figure 3-3: **μmedIC's Design.** An external reader powers up the micro-implant which harvests the RF energy, decodes commands, backscatters its response, and adapt its rate and configuration to channel conditions.

3.4.1 Resonant Rectenna Design

Before delving into μmedIC's design, it is helpful to understand the challenges that face RF energy harvesting inside tissues and how prior designs address these challenges.

Harvesting RF energy inside human tissues is more challenging than harvesting in air for two main reasons. First, RF signals exponentially attenuate as they traverse human tissues [31, 56], while in air, their amplitude decays linearly with distance. This makes it difficult for an external reader to deliver sufficient energy to power up an energy harvesting micro-implant inside tissues.[3] The second challenge facing in-body energy harvesting arises from the constrained form factor of micro-implants. Specifically, due to anatomical constraints, micro-implants have form factor requirements that vary between 2-3 cm [58] to sub-centimeter dimensions. The limited form factor makes it difficult to efficiently harvest energy since it constrains the dimensions of the micro-implant's antenna with respect to the wavelength of the RF signal [31].[4]

[3]Specifically, state-of-the-art RF rectifiers need around -34.5dBm of power to power up [57]. This minimum threshold is determined by transistor electronics.

[4]In the absence of such form factor requirements, achieving good radiation efficiency would require

Because of the above challenges, state-of-the-art proposals for in-body energy harvesting fine-tune their designs to optimize the harvesting efficiency along two main dimensions:

- *Radiation efficiency in Bio-tissues:* This refers to the efficiency of antennas in transmitting and receiving RF signals within a specific frequency band of interest. Because of the limited antenna form factor and the conductive properties of human tissues (modeled using the Debye model as explained in section 2.1), in-body antennas suffer from low radiation efficiencies (they are typically as low as 1%) [31]. In order to minimize losses due to the surrounding tissue environments, antenna engineers typically simulate their designs in electromagnetic simulators which account for the impact of the dielectric properties of tissues. This allows them to fine-tune various design parameters (like shape, geometry, thickness of conductor) to achieve the highest possible efficiency given the limited form factor and simulated medium [59].

- *Resonance:* Aside from optimizing the radiation efficiency of micro-implant antennas, state-of-the-art designs also exploit resonance [57, 60]. Resonance is a well-known electrical property that boosts harvesting energy efficiency by minimizing losses. It can be achieved by electrically matching the antenna impedance to the input impedance of the rectifier (energy harvester).

In order to maintain small form factor and optimize energy harvesting performance, state-of-the-art designs employ electrically small inductive loops, optimize their designs, and match them to the rectifying circuits [26]. The resultant rectennas are most efficient when they operate at their resonance frequency, defined by:

$$f = \frac{1}{2\pi\sqrt{L_A C_{rect}}} \tag{3.1}$$

antennas whose dimensions are of the same order of the wavelength [24].

where L_A is the inductance of the loop antenna and C_{rect} is the input capacitance of the rectifier.

3.4.2 The Impact of Tissues on Resonance

In our above discussion, we have maintained that it is possible to simulate in-body environments that reflect practical real-world conditions. While that is true in principle, it is very difficult to truly optimize the energy harvesting to reflect practical environments. This is because the human body consists of multi-layer tissues, each layer with a different depth. Moreover, the tissue composition changes across different individuals as well as different body parts or organs. This makes it infeasible to design a one-size-fits-all resonant rectenna that has high efficiency across different body parts (e.g., for mobile micro-implants), let alone for different humans.

The difficulty in adapting to complex tissues arises from differences in their relative permittivity ϵ_r (which reflect differences in the dielectric). Permittivity varies across different tissues, and directly impacts the antenna radiation pattern as mentioned earlier. For example, while the permittivity of muscle tissues is $\epsilon_m = 55 - 17.4j$, the permittivity of fat is $\epsilon_f = 11 - 2j$, both around the same frequency of 900 MHz which corresponds to the ISM band of interest [23].

To better understand the impact of such tissue variations on energy harvesting, recall Fig. 3-2 from the introduction which demonstrated how a design that is optimized to achieve high efficiency in muscle tissue within the ISM band (910 MHz) becomes inefficient at the same frequency when placed in a different tissue (e.g., fat). Indeed, we empirically verify this behavior in real-world measurements in section 3.8. This behavior demonstrates the difficulty in scaling prior rigid designs to complex tissue environments. Because of this lack of scalability, existing designs are limited to shallow depths, where the received energy remains sufficient to power them up despite their

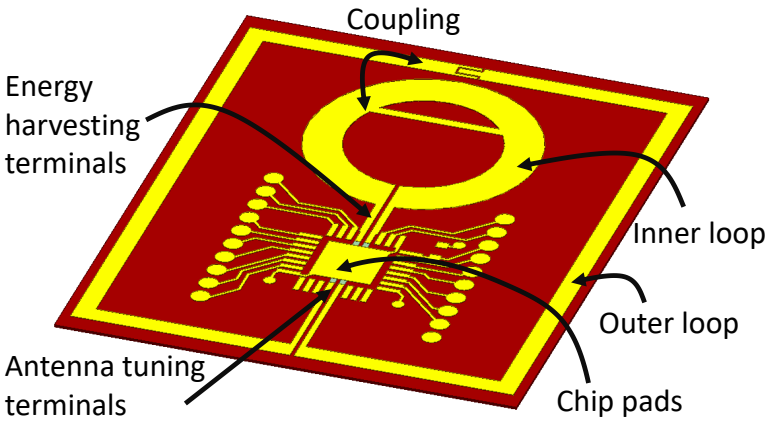


Figure 3-4: **Reconfigurable Antenna.** The proposed antenna design showing the inner loop, outer loop, coupling as well as chip ports for energy harvesting and reconfiguration.

low harvesting efficiency [19, 29].[5]

3.4.3 Reconfigurable Coupled Rectenna

To deal with the above challenges and scale to different in-body environments, μmedIC adopts a self-reconfigurable architecture that enables it to adapt to surrounding tissues. This reconfigurability is made possible by synergistically combining two sub-components: (1) the first is a reprogrammable antenna that can adapt its radiation efficiency to the surrounding medium, and (2) the second sub-component is reprogrammable matching circuit that enables shifting the resonance to ensure that the energy harvesting circuit and antenna remain matched. By tuning both the radiation efficiency and the resonance, μmedIC's design can adapt the two core dimensions that are typically pre-tuned to achieve high harvesting efficiency in tissues as per section 3.4.1. The rest of this section describes these two sub-components in detail.

Antenna Reprogrammability

To enable antenna reconfigurability, μmedIC employs a coupled antenna design. Recall that coupling refers to the interaction between two antennas when they are in close physical proximity [24], and is typically considered to be harmful. In our design, however, we exploit a coupled design in order to adapt μmedIC's radiation efficiency inside tissues. Technically, our goal is to change the current distribution along the radiating element in order to counteract the change in the surrounding medium's permittivity.

Fig. 3-4 shows μmedIC's coupled design, which consists of two loops: an outer rectangular loop and an inner circular loop (with a horizontal chord). Both loops interface with the IC, albeit for different purposes. The inner loop interfaces with the energy harvesting bank of the circuit (i.e., the rectifier) while the outer loop interfaces with the reprogrammability circuit which is implemented as a variable capacitor as we detail below. Because the two loops inductively couple due to their proximity, any change in the radiation pattern of the outer loop gets mirrored in the inner loop, thus changing its radiation pattern and allowing for programmability.

Next, we would like to understand how such a design allows shifting the radiation efficiency across frequencies. A standard approach for understanding an antenna's efficiency is to measure its input impedance. So, we simulated the input impedance of the inner loop and plot the real and imaginary part of that impedance across frequencies in Fig. 3-5. Each color in the figure represents a different configuration (i.e., a different capacitive load on the outer loop).

One approach to understand where an antenna is efficient is to look at the peak of the real component of its input impedance [24]. For example, right-most green curve has a peak around 900 MHz, indicating that the antenna is most efficient around

[5]At shallow depths, the RF signals experience less overall (exponential) attenuation due to a shorter path length inside tissues.

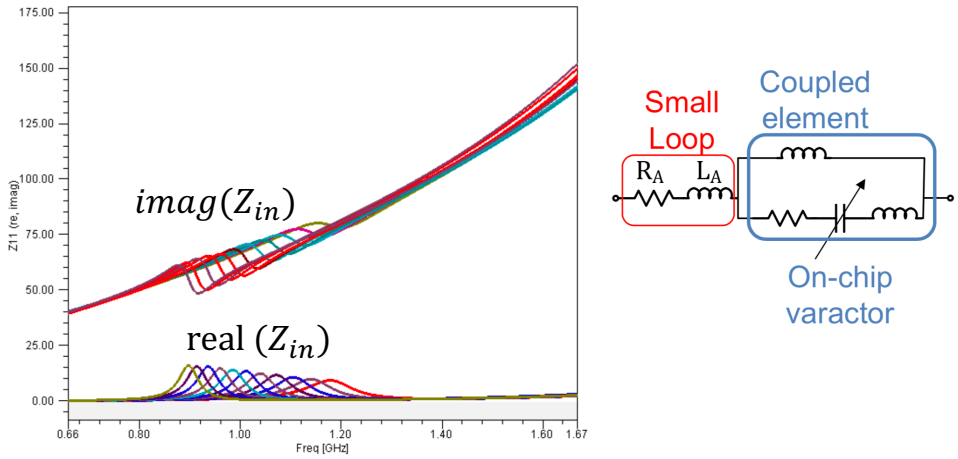
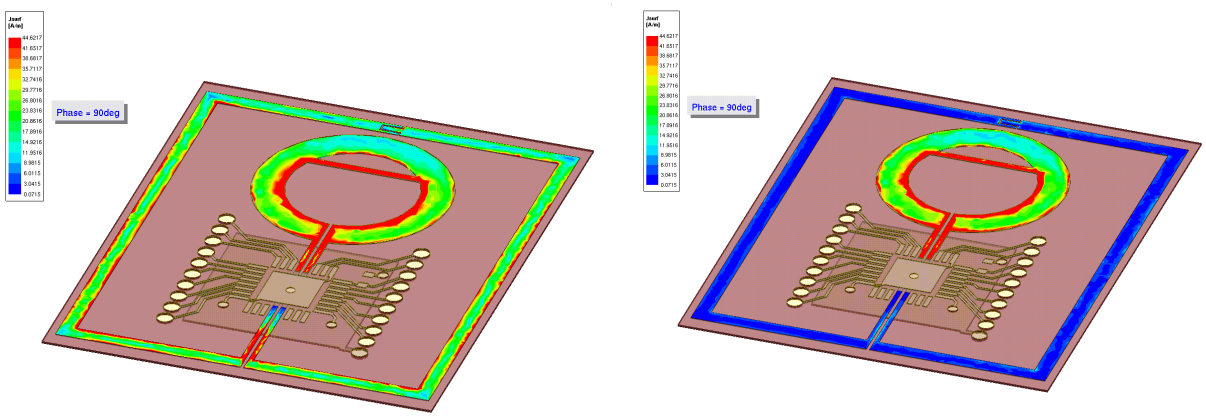


Figure 3-5: **Programmable Antenna Model.** The programmable coupled antenna can be modeled as an inductive loop coupled with a resonant LC tank (right figure) whose impedance shows a peak in the real part of its frequency response (left figure).

that frequency. However, as we change the load on the outer loop, that peak shifts, indicating that the frequency of highest radiation efficiency also shifts. This shows that μmedIC's design indeed enables programming the radiation efficiency. Such programmability is highly desirable because if the antenna becomes most efficient around 1.1 GHz due to surrounding tissues, this allows us to shift the highest efficiency region back to the 900 MHz ISM band.

The right side of Fig. 3-5 shows a conceptual schematic of the resulting coupled design, which is a standard approach to reason about coupled engineering designs [61]. The schematic represents the inductive coupling between the two loops as an inductor, and represents the programmability via an on-chip variable capacitor. In practice, we implemented this programmability as a switched capacitor bank for simplicity and energy efficiency. This schematic would exhibit the same behavior observed in the plots shown to the left as the capacitance is changed.

Therefore, in addition to the loop antenna, we incorporate an outer loop which couples with the internal loop to provide the higher order impedance matching. Additionally, the outer loop is loaded by a programmable capacitor bank to provide



a) High-coupling in fat tissue b) Low-coupling in muscle tissue

Figure 3-6: **Antenna Coupling** The figure shows how the coupling between the antenna radiating elements changes from one tissue (or frequency) to the other which necessitates the need for reconfiguration.

the antenna resonance tunability for operation in different tissues. The coupling intensity changes from one tissue to the other as illustrated in Fig. 3-6 where high coupling is achieved in a fat-based tissue but the same antenna has a lower coupling (different impedance and gain) in a muscle tissue. The capacitor bank is chosen such that the tuning range allows for retuning the antenna to achieve the same coupling in both tissues at the frequency of interest.

The antenna is simulated across different frequency ranges and inside different media (tissues) and multiple iterations are performed to reach an optimum design across the reconfigurability range.

Finally, we note that this programmable architecture was the result of many iterations in consultation with the relevant literature. Antenna design is an art and is known to require extensive iterations, especially for bio-tissues, and thus it remains an active area of research [59]. One of the interesting designs we explored consisted of a single loop, where one side of the loop wass connected to energy harvesting while the other was connected to a programmable load; such a design, however, had a much lower bandwidth than μmedIC's coupled architecture which resulted in significantly

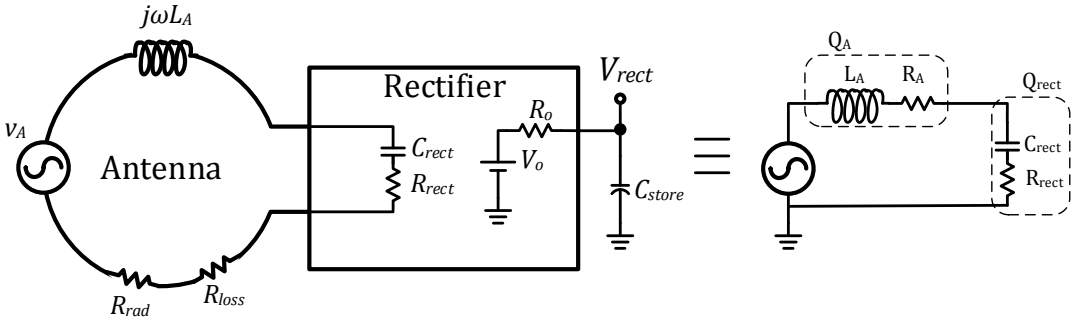


Figure 3-7: **Rectenna Circuit Schematic.** The rectenna can be modeled as a resonant LC circuit where the inductance is contributed by the antenna and the capacitance represents the rectifier impedance.

lower data rates.[6] Another interesting design element is the horizontal chord across the inner loop, which has also been recently demonstrated to achieve wider bandwidth and higher efficiency (albeit without reprogrammability) [57, 60]. Thus, because antenna design is a highly complex task, by introducing a simple design that enables reprogrammability, μmedIC can reduce the burden on pre-tuning all the parameters and allow for reconfigurability to adapt to different media.

Harvesting Reconfigurability

So far, we have focused only on improving the antenna's efficiency by shifting its resonance frequency. However, if we just do that, then we cannot ensure it remains matched to the energy harvesting circuit. Thus, we won't reap the benefit of resonance harvesting.

To optimize the energy harvesting efficiency, rectennas rely on the perfect resonance between an electrically small antenna with an inductive impedance profile with the conjugately matched capacitive input impedance profile of the rectifier circuit as shown

[6]Indeed, coupled designs are known to have larger bandwidth, and hence have been used in the design of wideband RFIDs and UWB front-ends [62, 63]. In contrast to prior coupled designs which are rigid, μmedIC's design allows for reconfigurability.

in Fig. 3-7. This can be expressed in the following complex equation:

$$Z_A = Z_{rect}^* \tag{3.2}$$

where Z_A is the antenna's impedance while Z_{rect} is the rectifier's input impedance. This can be expanded into the real and imaginary components:

$$\omega L_A = \frac{1}{\omega C_{rect}} \tag{3.3}$$

$$R_A = R_{rect} \tag{3.4}$$

where L_A is the antenna's inductance, R_A is the antenna's total resistance, R_{rect} is the rectifier's input resistance, and C_{rect} is the rectifier's input capacitance.

Now recall that in Fig. 3-5, the antenna programmability changes Z_A. So, we should change the rectifier accordingly to ensure resonance occurs at all programmable states.

To achieve this, we introduce programmable circuit matching. Since the programmable antenna is still an inductive one and the rectifier has a capacitive impedance, the required matching network can be implemented as a simple bank of capacitors. This capacitor bank can be used to compensate for the change in inductance from one state to the other, thus maintaining perfect conjugate matching. There is a direct trade-off between programmability and the quality factor of the network, and hence, the energy harvesting efficiency. Higher programmability requires more switches which adds more parasitic and degrades the overall performance, therefore, we choose a 6-bit programmable matching network compromising between programmability and efficiency.

Effectively, by reprogramming both the antenna and the harvesting circuit, we have disposed of the need to pre-fine-tune the design and allowed ourselves to retune it inside the human body. At design time, the antenna is simulated in different human

tissues and designed around a rough estimate to relax the tuning range specifications.

The guidelines for a systematic rectenna design approach for wirelessly powered integrated ultra-wide band transceivers is outlined in [26]. This approach utilizes an electrically small loop antenna whose input inductance and resistance are well controlled by the loop's radius as well as the wire's thickness. It then employs an iterative scheme in order to determine the optimal parameters for all the system components. The work in [64] provides a means of instantaneously varying the input impedance for near-field rapid charging, however, it doesn't provide programmability for far-field antenna operation.

One might wonder whether modifying the antenna alone or the energy harvesting alone might be enough. Implementing any of these approaches alone will lead to less desirable performance. Changing the matching alone can allow a slight shift in the center frequency (e.g., a slight shift in the channel) [65], but if the desired shift is too large, the antenna becomes inefficient. On the other hand, reprogramming the antenna alone would not be enough because it would significantly reduce the efficiency without resonance. It is by combining both of these techniques together that μmedIC can enable cross-tissue wireless and batteryless connectivity for micro-implants.

3.5 Rate Adaptation for In-Body Backscatter

So far, our discussion has focused on μmedIC's energy harvesting reconfigurability. Next, we discuss how it can adapt its bitrate to deal with varying channel conditions. Specifically, recall that μmedIC communicates on the uplink via backscatter. Moreover, it needs to support a variety of applications, some of which may require bitrates up to few Mbps (e.g., capsule endoscopes) [8]. Thus, it is desirable to enable the sensor to backscatter at the highest possible bitrate needed by the application of interest whenever possible. Below, we discuss the need for in-body backscatter bitrate

adaptation and how μmedIC's reconfigurable design can address these needs.

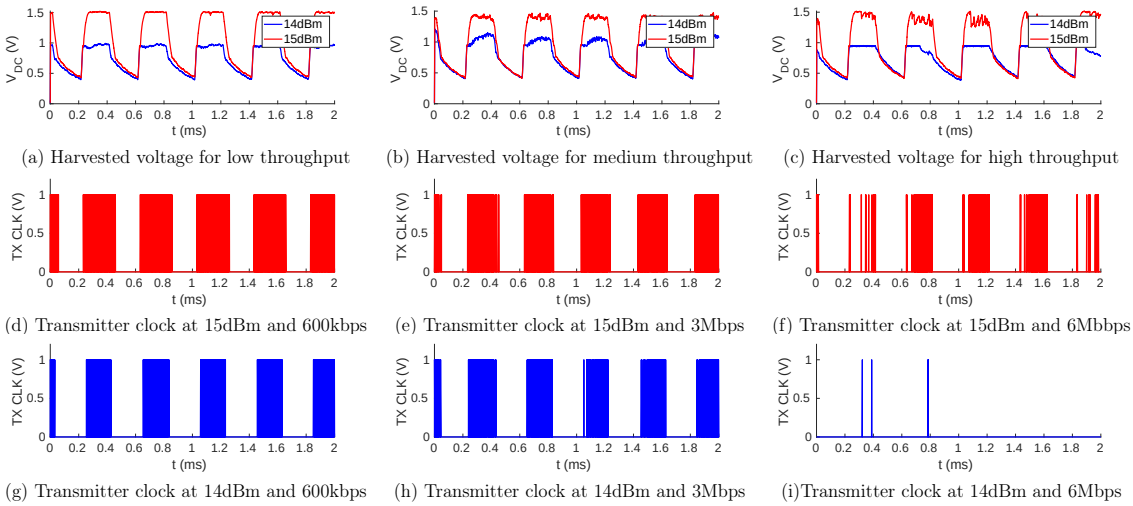
3.5.1 The Need for Adaptation

Bitrate adaptation is today a core component of a variety of wireless network protocols, including WiFi and LTE. It refers to the ability of certain communication devices to adapt their throughput to the channel conditions. For example, if the channel is strong (i.e., has high SNR), the communication link can sustain higher throughputs and the transmitter should use a higher bitrate since the channel capacity is higher. On the other hand, if the channel is weak (i.e., low SNR), the transmitter should transmit at a lower bitrate.

Bringing such bitrate adaptation to in-body micro-implants is desirable for two main reasons. First, as the person moves (or as the micro-implant moves inside the body), the wireless channel changes and the bitrate must adapt to it. A second, and equally important, reason arises from the relationship between power consumption and backscatter bitrate. Specifically, higher bitrates consume more power because the oscillator needs to be driven at a higher frequency.[7] (The overall power consumption P is directly proportional to bitrate f according to $P = fCV^2$ where C is the capacitance and V is the voltage.) Thus, the bitrate also needs to be adapted to the harvested energy to ensure that the micro-implant does not consume all its energy and die off.

To gain more insight into the trade-off between bitrate and power consumption, we ran experimental trials with μmedIC (implementation detailed in section 3.6). In each experimental trial, we pre-programmed the micro-implant to backscatter at a fixed bitrate. We repeated the experiment at three different bitrates (600kbps, 3Mbps, 6Mbps) and two different transmitted power levels (14dBm and 15dBm). We specifically selected two power levels that are close to demonstrate that μmedIC needs to adapt to changes as small as 1dB. In each experimental trial, the external reader

[7]Note that this bitrate frequency of the backscatter oscillator is different from the RF frequency of transmission.



(a) Harvested voltage for low throughput (b) Harvested voltage for medium throughput (c) Harvested voltage for high throughput

(d) Transmitter clock at 15dBm and 600kbps (e) Transmitter clock at 15dBm and 3Mbps (f) Transmitter clock at 15dBm and 6Mbbps

(g) Transmitter clock at 14dBm and 600kbps (h) Transmitter clock at 14dBm and 3Mbps (i)Transmitter clock at 14dBm and 6Mbps

Figure 3-8: **Availability vs Bitrate and Power Level.** The figure plots the availability of μmedIC's communication as a function of different bitrates and power levels. The different columns represent different throughputs in increasing order from left to right (600kbps, 3Mbps, 6Mbps); the colors represent different transmit powers (blue for 14 dBm and red for 15 dBm). The top row represents the voltage harvested over time for the two power levels. The middle and bottom row show the periods in time with the sensor is on (1V) and off (0V).

is programmed to alternate between transmitting for $200\mu s$ and pausing (i.e., not transmitting anything) for $200\mu s$. In each trial, we measured μmedIC's harvested DC voltage and the internal ring oscillator's clock voltage over time.

Fig. 3-8 plots the measured voltages across the three different fixed bitrates and the two power levels.

We make the following remarks:

- The harvested voltage in Fig. 3-8(a)-(c) at the higher power is larger when the transmitted power by the external reader is 15dBm (red plot) than when the transmitted power is 14dBm (blue plot). This is expected since higher power leads to more harvested energy.

- In the high-transmit-power low-rate regime (Fig. 3-8(d)), μmedIC is able to continuously backscatter for the entire duration that the external reader is on; in fact, the node has enough energy to backscatter for a longer duration, even after

the external reader is turned off (due to the excess harvested energy). Moreover, even in the lower power regime (Fig. 3-8(g)), it can backscatter almost for the entire duration of the external reader's transmission.

- At the other extreme, when μmedIC is programmed to the higher rate of 6Mbps, it can only power up at the higher reader power, and even then, it only transmits continuously for 20 – 50μs before the oscillator dies off to recharge again, causing the duty-cycled operation shown in Fig.3-8(f). When the reader's power is lower, it can't power up or oscillate steadily as depicted in Fig. 3-8(i).

- Finally, the medium rate of 3Mbps sits at a sweet spot where it can achieve higher overall throughput while maintaining the ability to power and continuously transmit without frequently dying off during backscatter.

In principle, one could preprogram the micro-implant to conservatively backscatter at the lowest bitrate. However, this would not be desirable as it would forgo the opportunity to enable higher throughput. In the next section, we describe how μmedIC can adapt its rate to the available energy.

3.5.2 Throughput Programmability

In order to take advantage of good channels, and at the same time, not die off at low channels, μmedIC performs bitrate adaptation. The standard approach for bitrate adaptation is to wait for the receiver to transmit acknowledgment packets. However, such approach is undesirable for multiple reasons. First, we want to adapt the bitrate *before* the sensor dies off. Second, the overhead for waiting for an acknowledgment results in unnecessary loss of harvested energy [51].

To close the loop on bitrate adaptation, μmedIC monitors circuit level sensor hints. Specifically, it senses the harvested voltage and preemptively adapts its bitrate before dying.

Next, we describe how this can be realized in practice. μmedIC's backscatter switch is driven by a digitally controlled oscillator. The oscillator's frequency can be in one of eight different states (i.e., 3 control bits). By employing a current-starved ring oscillator architecture, we can digitally tune its frequency by injecting more current to the ring oscillator in order to increase the frequency or by starving the core ring so that a lower frequency can be attained. The rectenna tuning logic senses the DC voltage and incrementally increases or decreases the oscillator frequency. This frequency is used to modulate and encode the sensor bits and backscatter to the reader. Alg. 1 summarizes this algorithm, where V_{DC}, V_{TH}, and D_{fosc} represent the harvested voltage, turn-on threshold, and oscillator's frequency configuration respectively.

Algorithm 1 Incremental rate adaptation

SENSE THE VOLTAGE:
Sense stored voltage V_{DC}
LEARN THE STATE:
Convert V_{DC} into a 3-bit code $D_2D_1D_0$
RECONFIGURE THE OSCILLATOR:
if $V_{DC} > V_{TH}$:
    Increment the frequency: $D_{f_{osc}} \leftarrow D_{f_{osc}} + 1$
else:
    Decrement the frequency: $D_{f_{osc}} \leftarrow D_{f_{osc}} - 1$
REPEAT VOLTAGE SENSING

Few additional points are worth noting:

- So far, we have described μmedIC's bitrate adaptation algorithm. The same idea can be extended to resonance adaptation as shown in Fig. 3-9. Specifically, by sensing the harvested voltage using a sampler (ADC), the node can apply stochastic gradient descent to move to a more efficient harvesting state by updating the matching circuit and resonance capacitance. It is worth noting, however, that unlike rate adaptation, resonance and matching adaptation require the off-chip storage super-capacitor to have some residual energy in the first place. This "warm-start" approach is a standard assumption in the design of

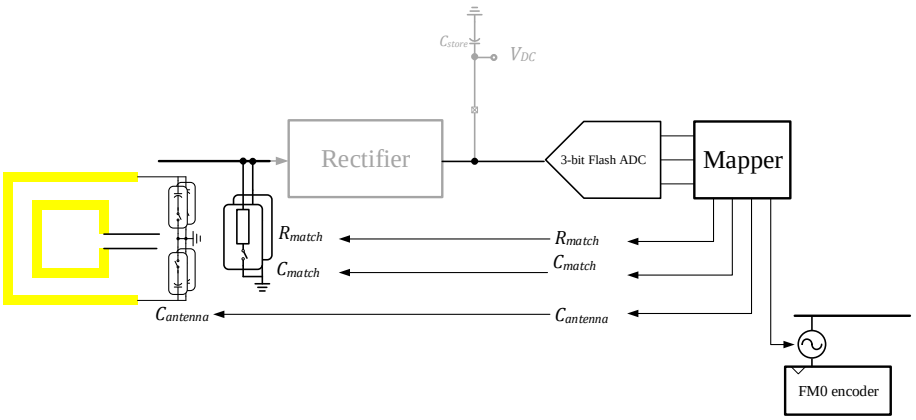


Figure 3-9: **Self-Reconfiguration Logic.** μmedIC samples the stored DC voltage and maps it to discrete values for the antenna configuration, matching state, and bitrate.

energy harvesters [60]. Extending the design to cold-start is beyond the scope of this work.

- There are three types of reconfiguration parameters (matching capacitor bank, resonance capacitor bank, and oscillator frequency). Each of these parameters can be reconfigured independently. The two capacitor banks can be adapted on a packet-by-packet basis. In the simplest implementation, we alternate between incrementing/decrementing each of the two capacitor banks. Looking ahead, it would be interesting to explore more optimal algorithms that can leverage μmedIC's reconfigurable design to achieve higher throughput than our simple adaptation algorithms.

- Our discussion has focused on rate and resonance adaptation. However, μmedIC's design extends to decoding packets on the downlink (via PIE encoding) and encoding backscattered packets on the uplink via FM0 encoding similar to RFID communication. The ability to decode downlink packet enables the reader to employ a master-slave Medium Access Control (MAC) protocol and extend to multiple micro-implanted sensors concurrently.

- In our evaluation, we noticed that the backscatter bitrate varied over time, even when the oscillator was expected to transmit at a fixed rate. This was caused by the susceptibility of the node's ring oscillator to environmental variables. To deal with this issue and decode correctly, our reader continuously tracks the backscatter frequency and adapts to its variations. Practically, this was implemented via a bit-by-bit maximum likelihood decoder that corrects phase/frequency errors incrementally from one bit to the other.

In sum, the rate adaptation operates on a packet-by-packet basis where the chip senses the voltage and increments or decrements the bitrate accordingly. On the receive side, the reader uses the preamble of the backscattered packet in order to determine the backscatter rate and correctly decode the sensor's data.

3.6 IC Design & Antenna Fabrication

ASIC Implementation. μmedIC is implemented as an application-specific integrated circuit (ASIC), whose prototype is shown in Fig. 3-1.The ASIC incorporates the entire system-on-a-chip, and integrates all the antenna and circuit programmability, logic, and communication functionality onto a single chip. The chip layout is divided into multiple blocks which was taped-out and fabricated in a 65nm TSMC CMOS RF-LP process. The magnified die photo is shown in Fig. 3-11 where the chip occupies an area of 1×1 mm^2. The figure also highlights the capacitor banks for the tunable input impedance matching as well as the antenna reconfiguration, the energy harvesting blocks, LDO, the receive and transmit chains, and finally, the logic that controls the full operation.

Coupled Antenna on Flexible Substrate. The ASIC is wire-bonded to the coupled antenna structure on a printed antenna on a flexible PCB. The programmable coupled antenna consists of two microstrip copper loops. The two coupled loops enable

reconfiguration of the antenna centered around ISM band (902 - 928MHz) with a flexibility range around 200MHz. The flexible PCBs were simulated in High-Frequency Structure Simulator (HFSS) [66] and fabricated by FlexPCB [67].

The chip and the antenna flexible board are encapsulated in a biocompatible polymer (Ecoflex polymer) to mitigate any reaction with the human tissues and insulate the node from the harsh in-body environment.

Note that while our final evaluation was performed with flexible substrate, we have also successfully tested the ASIC with different antenna designs and on rigid substrates including FR-4. The overall antenna design went through multiple iterations where we compared the impedance in simulation to that measured using a network analyzer.

Overall Architecture and Energy Harvesting. The integrated system block diagram is depicted in Fig. 3-10 which consists of the rectifier, the power management unit (PMU), the rectenna tuning logic, the receiver chain, the transmitter chain, and other auxiliary blocks. The energy harvesting chain incorporates a 6-stage differential rectifier with a self-V_{th} cancellation technique to generate a constant voltage over an off-chip storage capacitor using the CW RF input signal. The chip employs a cross-coupled six-stage rectifier as shown in Fig. 3-12. Following a rectenna design procedure, the capacitor values as well as the transistor sizing are co-optimized with the antenna dimensions in order to guarantee impedance matching and high quality factors for optimized energy harvesting efficiency.

Then the role of the power management unit (PMU) is to limit and regulate the harvested voltage in order to provide a stable supply for the more sensitive communication circuits and logic. The PMU was implemented using a voltage limiter and a low-dropout regulator (LDO) to provide regulated power supply to the rest of the circuit.

Power Management Unit. The power management unit (PMU) is illustrated in Fig. 3-13 where the rectifier's output voltage V_{rect} is stored over a storage capacitor

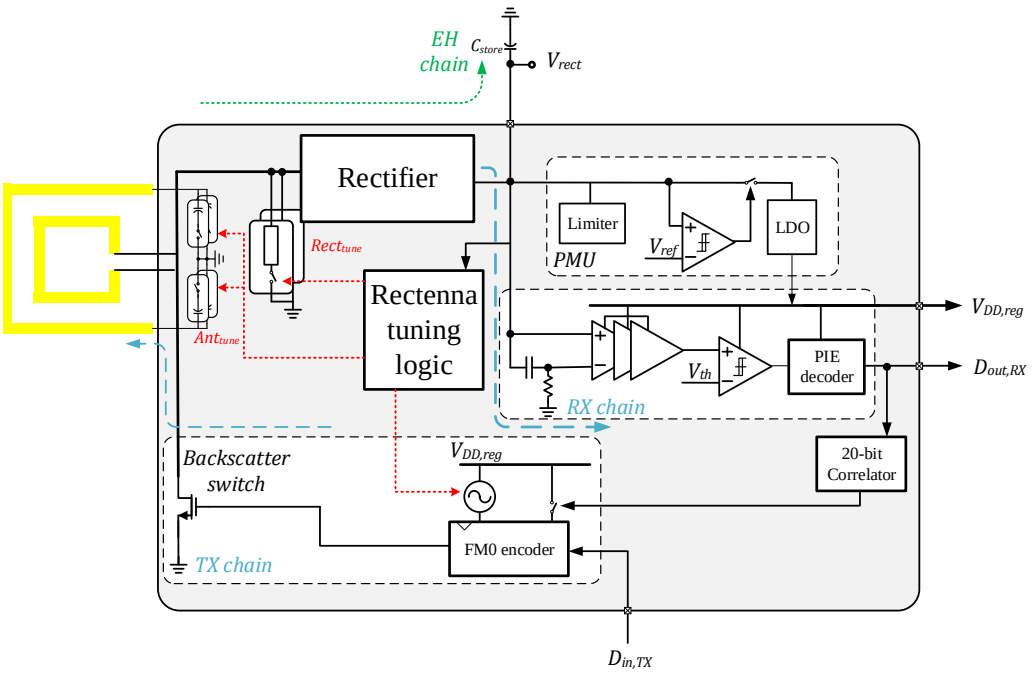


Figure 3-10: **μmedIC's Chip Block Diagram.** The chip consists of energy harvesting and power management building blocks as well as receive and transmit chains. The tuning logic controls the chip's configuration as well as the system's state of operation.

C_{store}. This voltage then feeds a voltage limiter to prevent the circuit from reaching breakdown voltages while a voltage comparator turns on the low dropout regulator (LDO) once the V_{rect} crosses a reference voltage of $0.7V$. The LDO then provides a stable supply for the rest of the chip and triggers a Power-on-reset (PoR) signal to reset all the finite state machines (FSMs) as well as the flip flops for the different configuration bits.

The low dropout regulator (LDO) is designed as a negative feedback system with a differential pair error amplifier which is used to maintain a fixed voltage while a PMOS pass transistor provides the necessary current for the rest of the chip. The LDO output voltage is set by the resistor divider ratio and a RC load adds a zero to the transfer function to improve the phase margin of the feedback loop, and hence, its stability.

Receive Chain. The communication protocol in this system adopts a similar protocol

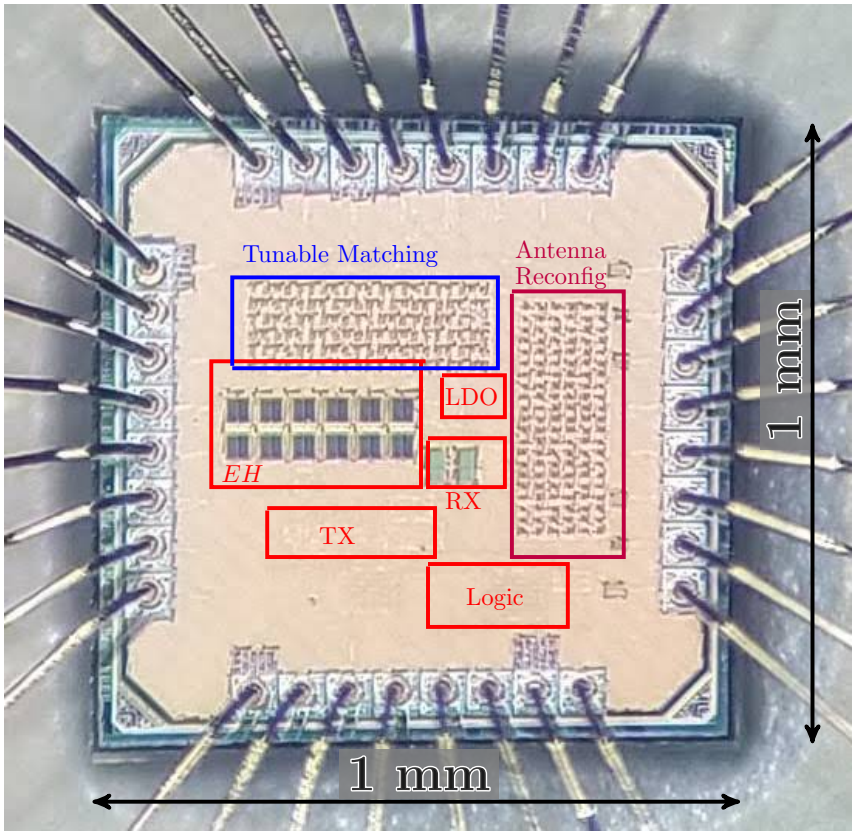


Figure 3-11: **μmedIC's Diephoto.** A 1×1 mm^2 CMOS chip was fabricated in a 65nm CMOS process and integrated with a custom microstrip printed antenna on a flexible PCB.

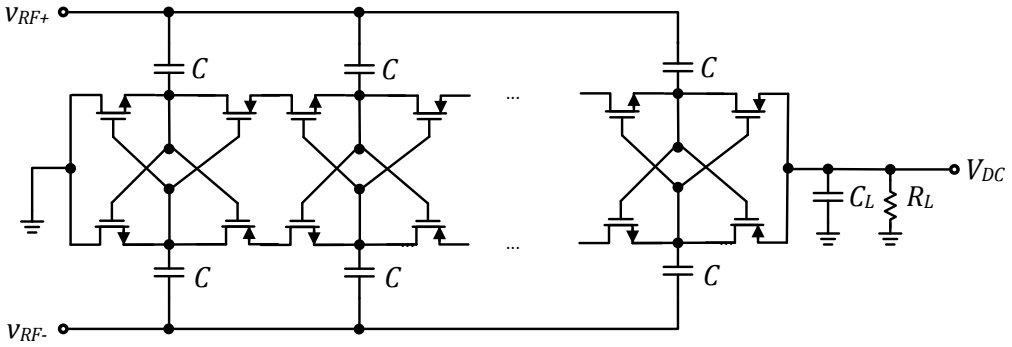


Figure 3-12: **Cross-coupled rectifier.** A N-stage cascading of self V_{th} cancellation architecture is adopted for the lowest sensitivity.

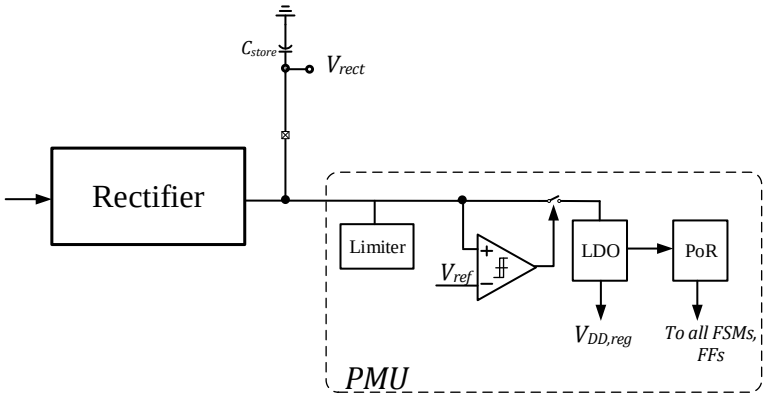


Figure 3-13: **Power Management Unit.** The power management blocks provide voltage limiting, voltage regulation, as well as reset signals for the entire chip logic.

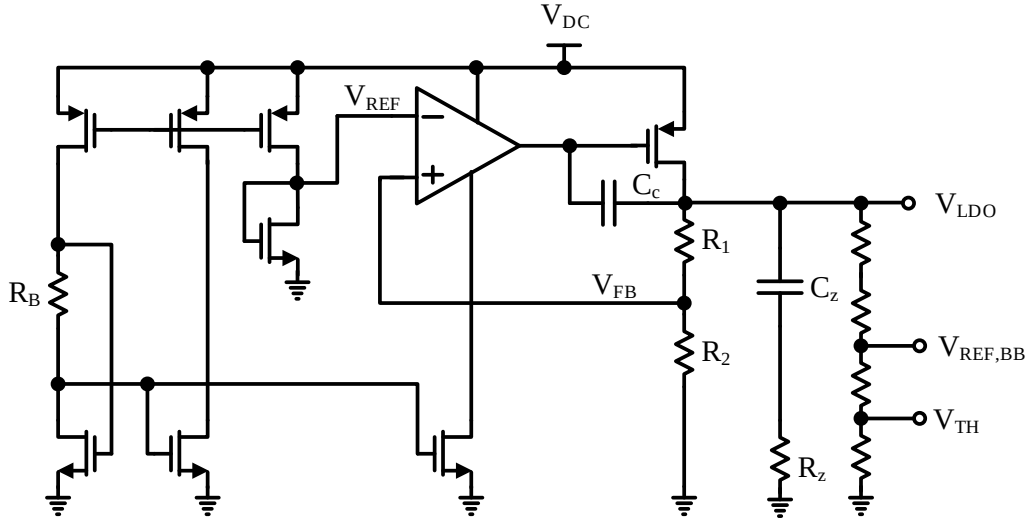


Figure 3-14: **Low Dropout regulator.** The figure shows the schematic for the LDO which utilizes a PMOS pass transistor to provide the load current and an RC load for compensation.

to the RFID standard [68] where the reader uses the downlink to power up the node as well as to transmit a double side band amplitude shift keying (DSB-ASK) modulated packet with a pulse interval encoding (PIE) while the uplink employs backscattering to transmit an ASK modulated signal with an FM0-baseband encoding back to the reader.

The input modulated signal follows the receiver chain where it gets amplified, filtered and demodulated. Then, it passes through a decoder which converts the Pulse Interval Encoded (PIE) symbols into output bits. Finally, a 20-bit correlator correlates the received packet MAC address to a stored 20-bit sequence to determine whether this packet is addressed to it or to another implant. The incoming RF envelope is modulated according to Fig. 3-15 such that both bits experience a transition with the pulse width for the low level (PW) while bit-0 has a an overall smaller bit duration ($T_0 < T_1$). In this design, T_1 and T_0 are chosen such that the on-duration of bit-1 is twice the on-duration of bit-0.

The decoder employs and integrate-and-dump mechanism to decode the incoming signal as illustrated in Fig. 3-15 where the '0' bits have a shorter on-duration, and hence, accumulate a smaller value at the end of the pulse while the '1' bits accumulate almost double the voltage triggering a comparator to give a '1' when the threshold voltage (V_{TH}) is adjusted in the middle between the length of the two pulses.

The overall receiver circuit is shown in Fig. 3-16 where a coupling capacitor (C_c) couples the ac envelope of the signal while a biasing resistor (R_B) sets the bias of the following amplifiers. A Schmitt-triggered buffer generates the clock signal to sample the integrator output while the integrator is designed as a passive switched capacitor integrator with a fixed current source.

Transmit Chain. On the uplink side, once a full correlation is achieved, the regulated supply turns on a tunable ring oscillator which generates the clock signal for an FM0 encoder and a data sampler to provide the modulating signal for the backscattering

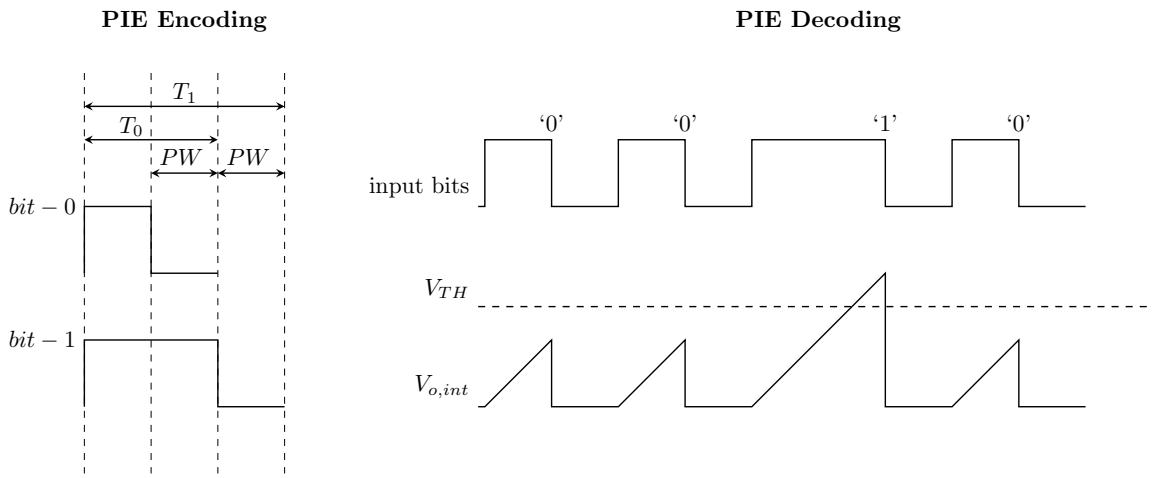


Figure 3-15: **PIE encoding and decoding.** The figure shows the pulse-interval encoding scheme employed on the downlink as well as the proposed decoding scheme for data recovery.

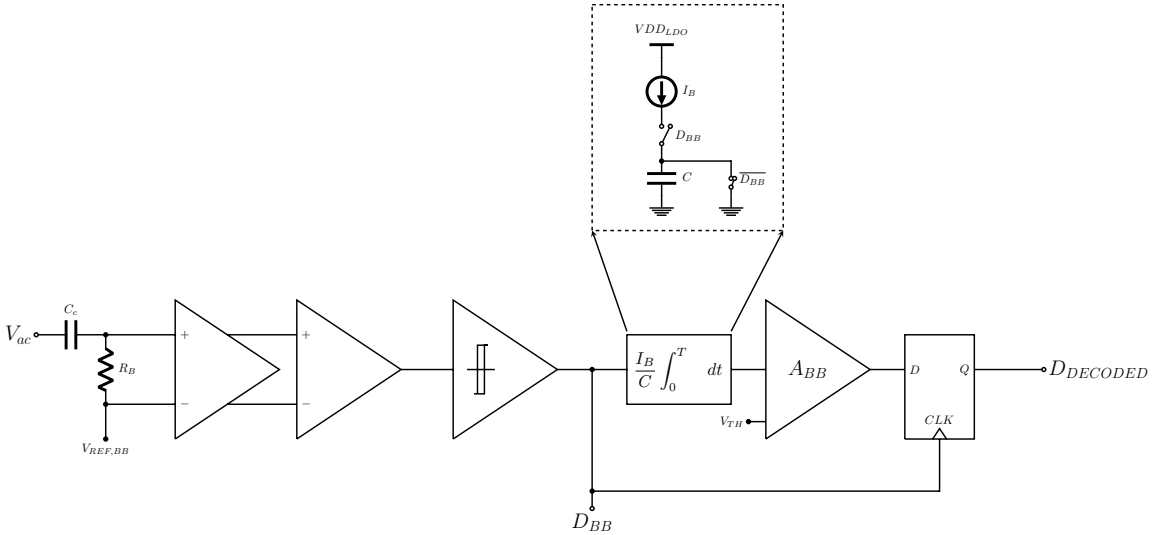


Figure 3-16: **Receiver chain.** The receiver employs an integrate-and-dump decoding scheme where the '1' bit is longer than the '0' bit in the downlink path.

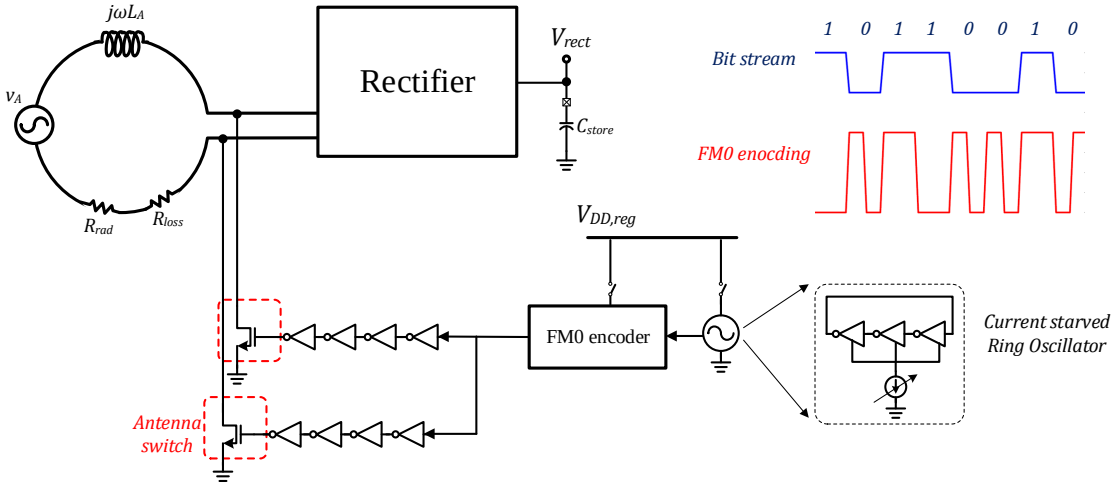


Figure 3-17: **Transmitter chain.** The transmitter utilizes differential backscattering switching and a ring oscillator for a programmable rate with an FM0 encoder.

switch, completing the whole transmitter chain. We implemented the oscillator as a digitally controlled 6-bit current-starved ring oscillator which is used to control and gracefully adapt the backscatter rate of the micro-implant. The oscillator can sustain up to 20 Mbps throughput; however, the rate adaptation limits it to 6 Mbps.

In the transmitter chain, antenna switches are used to modulate the reflection coefficient of the node between two absorptive and reflective states. The schematic for the transmitter is shown in Fig. 3-17 where a current-starved digitally controlled ring oscillator (DCO) is used to provide an adaptive datarate for transmission while an FM0 encoder is adopted to encode the incoming raw input bitstream. The state machine for such encoding scheme is further illustrated in Fig. 3-18 where the encoding ensures that there is always a transition between bits and bit-0 experiences an extra transition in the middle of the symbol while bit-1 has a fixed envelope for the bit duration.

Reconfigurability. For the rectenna reconfigurability logic, we implemented dual capacitor tuning for resonance as well as harvesting reprogrammability. The chip utilizes two 6-bit capacitor banks, each of which has 64 discrete capacitor values. Both

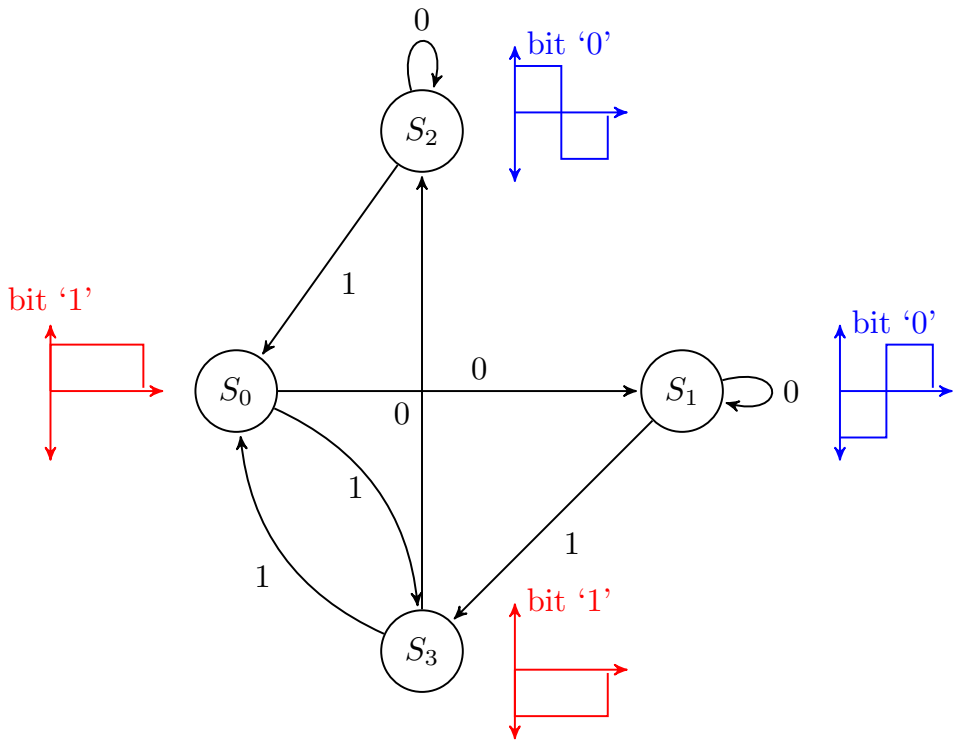


Figure 3-18: **FM0 encoding state machine.** The encoding dictated by FM0 must have a transition between bits while the '0'-bit has an extra transition in the middle.

capacitor banks are implemented as binary weighted capacitors connected to the inner or outer loops of the antenna through individual selection switches with a maximum tuning of 1pF. For the antenna resonance tuning, the capacitor bank is connected to the differential load terminal of the coupled antenna. For the rectifier harvesting tuning, the capacitor bank is connected in parallel with the rectifier in order to tune the input impedance of the chip. In order to provide an adaptive operation across different in-body tissue operation and cross-tissue connectivity, the chip has to be able to adapt its input impedance as well as tune the antenna to maintain a high energy harvesting efficiency for powering up.

The programmable input matching is incorporated in the rectifier front-end as shown in Fig. 3-19 where a differential capacitor bank is added between the RF terminals to tune the overall capacitive input impedance of the chip.

Logic Unit. The state machine for the proposed chip starts with the *Charge* state

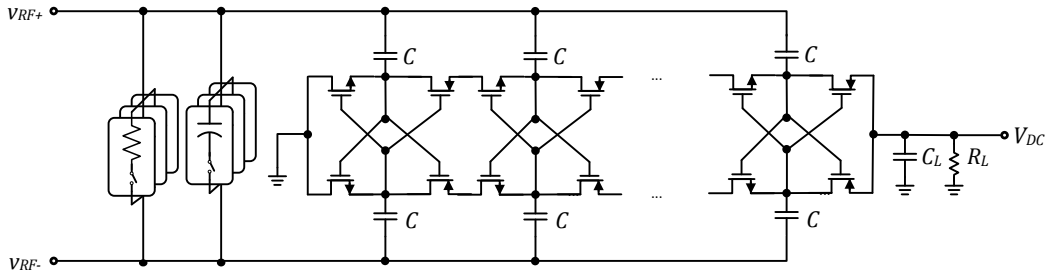


Figure 3-19: **Programmable Matching Cross-coupled rectifier.** The RF front-end of the rectifier employs a programmable bank of passive elements to reprogram the input impedance.

where the rectifier performs RF to DC conversion by charging the storage capacitor. The logic goes through the states outlined in Fig. 3-20, once the chip powers up, the receiver is turned on and starts to correlate with a pre-determined preamble. If the correlation flag is high, the re-configuration logic is initialized by sampling the stored DC voltage and mapping it to different values for the input impedance matching (C_{match}), the antenna resonance reconfiguration through (C_{tune}) as well as the datarate which is controlled by the ring oscillator (DCO). Finally, it switches to the TX state where the FM0 encoder is turned on to produce the encoded bitstream to the backscatter switch untill a full packet is transmitted triggering a TX_{done} flag to become high.

A schematic of the circuit operation of the reconfiguration logic is shown in Fig. 3-21 where the stored voltage (V_{DC}) is scaled and sampled then level shifted to the LDO voltage (V_{LDO}) before passing through the 3-bit Flash ADC and into the matching/tuning mapping block.

3.7 Evaluation

We evaluated μmedIC across five kinds of in-body environments including: minced meat, fatty tissues, mixed tissues with bone, saline water, and oil-based fluids. Since

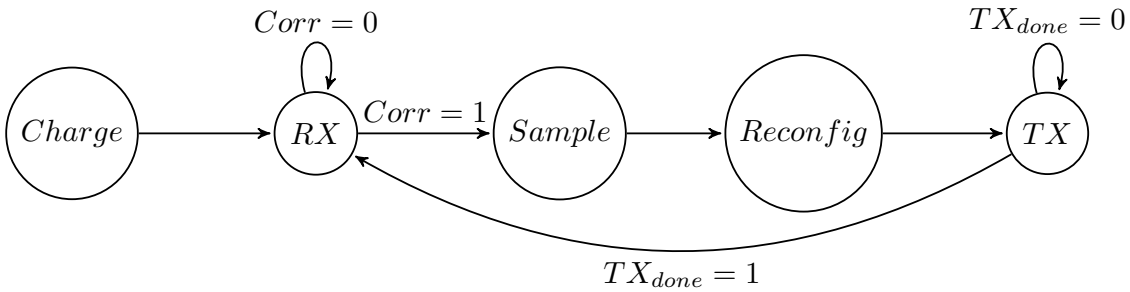


Figure 3-20: **State Machine.** μmedIC's state machine starts with the Charge state, moves into the receive state, then reconfigures before transmission via backscatter.

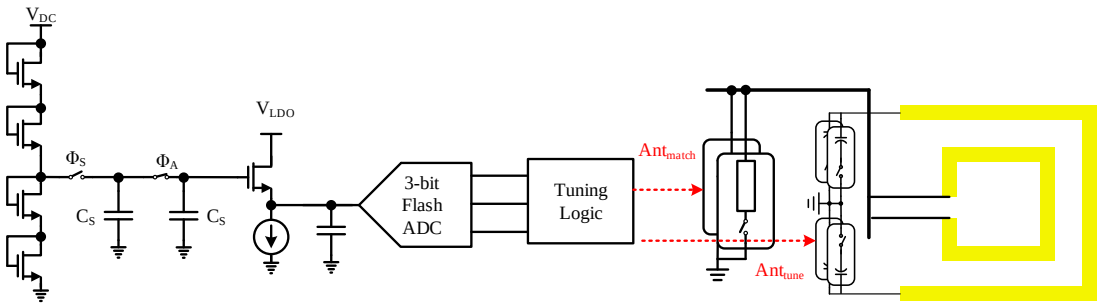
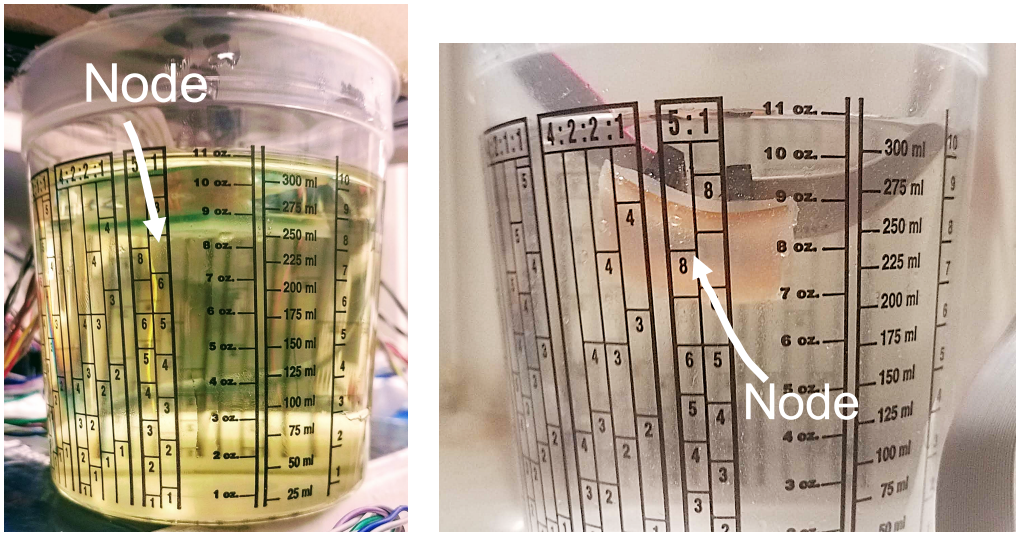


Figure 3-21: **Self-tuning Logic.** The harvested DC voltage is scaled and sampled by a 3-bit ADC then mapped to different configurations for the antenna resonance and input impedance matching.



(a) Oil-based setup (b) Saline water-based setup

Figure 3-22: **In-vitro test setups for μmedIC.** The figures show test setups in: (a) an oil-based fluid and (b) a saline-water fluid setup.

the majority of human tissues are oil-based or water-based, this allows us to cover a large variety of potential environments and multi-layer tissues. In each of these environments, we either submerged the sensor entirely in the fluid, shown in Fig. 3-22 or covered the antenna with meat tissues as in Fig. 3-23. In addition to the different tissues, we evaluated our setup at different transmit powers, orientations, as well as distances ranging from 10cm (between the reader and the tissue with μmedIC) at low power levels to almost a meter at a transmit power of 20dBm. The pins of the IC are connected via a 1.27mm pitch bus to a Tektronix MSO3054 oscilloscope and to an FPGA to allow for testing and voltage measurements. Note that our design allows bypassing the self-reconfigurability to allow for external configurability and testing each state independently. Moreover, an Agilent N9020A spectrum analyzer [69], hooked directly to an antenna, was used to initially characterize the backscatter modulation depth at different rates and center frequencies.

Subsequently, our complete end-to-end evaluation was performed using a software radio setup which employed two USRP N210 [70] boards for collecting and post-processing a large number of packets and estimating the BER under different channel

(a) Mixed tissue (b) Lean tissue (c) Fatty tissue

Figure 3-23: **Ex-vivo test setups for μmedIC.** The figures shows test setups in: (a) a mixed tissue, (b) a lean meat tissue, and (c) a fatty tissue.

conditions. One USRP board (with an SBX daughterboard [71]) served as the transmitter for the micro-implant, powering the chip up and providing downlink commands. The other USRP (with LFRX daughterboard [72]) worked as the reader, capturing the backscatter signal at a sampling rate of 25MSps. Both USRP boards were synced together using the same reference clock of 10MHz of a CDA-2990 Octoclock 8-channel distribution module [73]. Moreover, their front-ends were connected to log-periodic antennas [74] and their backends were connected via ethernet cables to allow for a central Linux machine to control both of them simultaneously. The data was then collected and post-processed using MATLAB to characterize the bit error rate, SNR, throughput and availability in the different tissues under test.

3.8 Performance Results

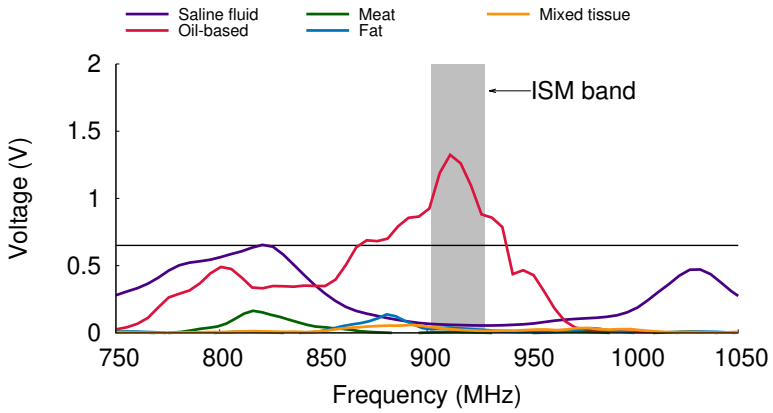
In this section, we report the evaluation results of μmedIC's performance in real-world environments and various in-tissue conditions.

3.8.1 Energy Harvesting

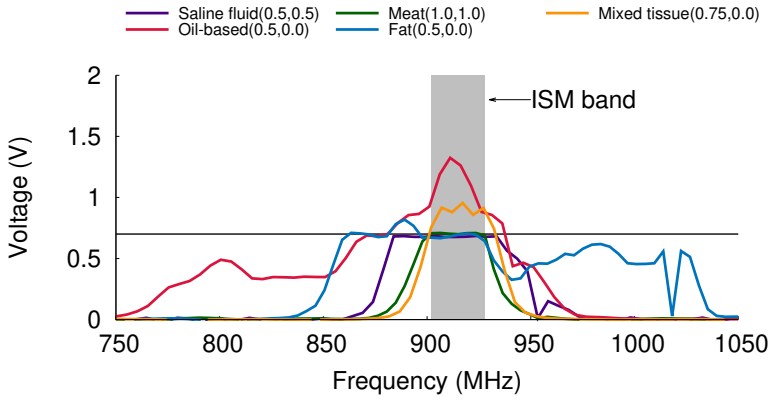
First, we evaluated μmedIC's ability to harvest energy across a variety of in-tissue environments. To do this, we used the Keysight N5183 MXG signal generator [75] as an RF source with fixed transmitted power. The signal generator was connected to a wideband log-periodic antenna covering the range of interest. We swept the transmitted frequency and recorded the received signal using an oscilloscope hooked up to the storage capacitor pin of μmedIC.

Fig. 3-24(a) shows the harvested voltage of a *rigid design*, i.e., when the tuning capacitor (of the antenna) and the matching capacitor are fixed. The figure plots the harvested voltage as a function of the frequency of the signal transmitted by the reader. We repeated the same measurement across the five tissue environments described in section 3.7 with testing depths of around 10cm or less. The figure also plots a solid black line around $0.65V$, which indicates the minimum voltage required to turn on the low drop-out voltage regulator (LDO). The figure shows that for this fixed configuration, the micro-implant can be powered up in the ISM band only when it is placed in the oil-based tissue (red curve), where the harvested voltage is above the minimum threshold. For all other tissues, the peak is either shifted outside the ISM band (shaded grey region), or the rigid design is completely unable to power up due to low efficiency.

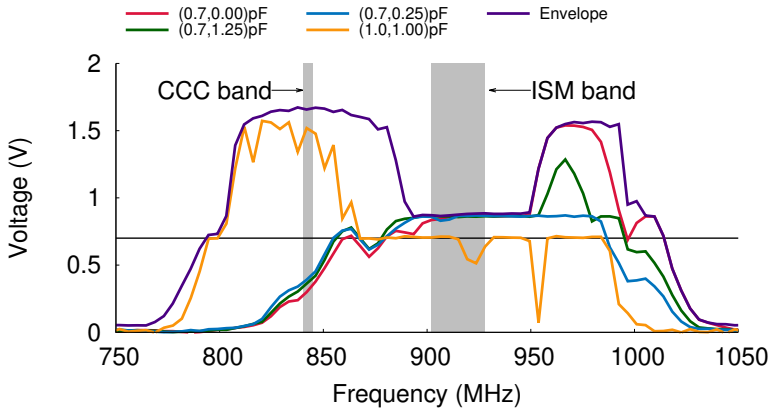
Next, we were interested in assessing whether μmedIC's reconfigurability allows it to power up in the ISM band. So, for each tissue environment, we looped through all 4096 configurations (changing the tuning and matching capacitors). For each tissue, we chose the configuration that has the highest harvesting voltage in the UHF ISM band. Fig. 3-24(b) plots the resulting curves. The figure shows that across all tissues, μmedIC can harvest enough energy inside the UHF ISM band to power up (the harvested voltage is at or above the threshold). It also shows that the optimal configuration for energy harvesting is different across tissues. For example, optimal



(a) Single Rigid Configuration



(b) Optimal Configurations in ISM band



(c) Envelope of Configurations in Oil-based

Figure 3-24: **Energy Harvesting in Tissues.** The figure plots the harvested DC voltage as a function of frequency across: (a) different tissues for a single rigid chip configuration, (b) different tissues while programming for the optimal configuration in the ISM band, (c) a fixed oil-based tissue while choosing the highest energy harvesting configuration to cover the widest bandwidth (shown by the envelope contour in purple).

powering up in saline fluid can be achieved at with a matching capacitor $C_m = 0.5pF$ and a tuning capacitor $C_t = 0.5pF$; however, optimal powering in mixed tissue requires $C_m = 0.75pF$ and $C_t = 0pF$. This demonstrates that both the antenna and matching programmability are necessary to adapt to different tissues.

Next, we were interested in understanding the extent of reconfigurability of μmedIC's harvesting efficiency. This time, we fixed the tissue to an oil-based medium, and we looped again through all the configurations. For each frequency between 750 MHz and 1050 MHz, we chose the configuration that yielded the highest harvested voltage. Fig. 3-24(c) plots the envelope of these peaks across frequencies (in purple) as well as a sample subset of configurations. The figure shows that the peak indeed moves across different configurations by up to 200 MHz. Such range of frequency shift is desirable as it allows us to also exploit other bands.

Finally, we were interested in investigating whether deforming the antenna impacts is resonance (e.g., rolling it as a pill). Our experimental evaluation verified that such deformation may indeed shift the energy harvesting peak by up to 60 MHz. Moreover, similar to our earlier demonstration, μmedIC's reconfigurability enables shifting the resonance back to within the ISM band.

3.8.2 Rate adaptation

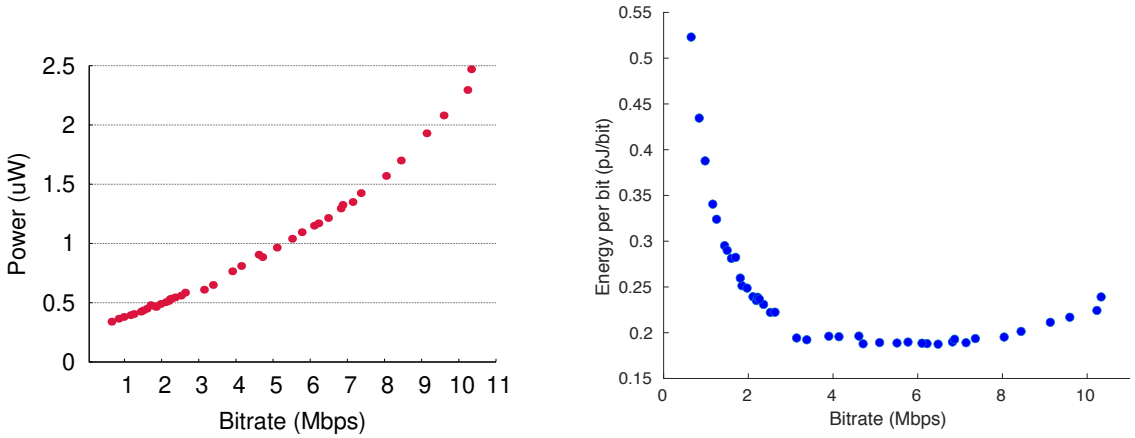
Next, we wanted to assess the second dimension of reconfigurability in μmedIC's design, namely its bitrate adaptation. Recall that bitrate adaptation is necessary to allow adapting to different channel conditions as well as harvested power levels, as highlighted in section 3.5.

(a) Power Consumption vs Throughput. First, we were interested in measuring μmedIC's power consumption as well as the impact of throughput on it. To perform this evaluation, we connected the IC to an external power supply of $0.5V$ rather than to its internal LDO and we measured the current drawn using the Keithly 2400

sourcemeter [76]. We repeated the same measurement at different clock frequencies (i.e., throughput).

Fig. 3-25 plots the average power and energy per bit consumption against the transmitter bitrate where the lowest configuration oscillates at a rate of 600kHz while consuming power as low as 340nW. On the other end, when the available input RF power is high, the node can trade-off its power consumption for a higher bitrate up to 10Mbps at the expense of 2.5μW of power. Therefore, with an adaptive scheme, the node can scale its datarate as well as power consumption by an order of magnitude according to the available power. While if we are interested in the transmission efficiency, the node can scale its energy per bit towards compromising between throughput and power consumption.

(b) BER-Throughput Curves. Next, we were interested in assessing the importance of bitrate adaptation to deal with varying channel conditions. We ran 90 experimental trials in total. In each experimental trial, we fixed the backscatter bitrate and the transmit power (of the external reader), and we transmitted for a fixed duration



(a) Power consumption (b) Energy consumption per bit

Figure 3-25: **Power and Energy Consumption vs Bitrate.** The figure plots (a) the average power consumption against the bitrate, showing that higher bitrates consume more power, and (b) the energy per bit as a function of the bitrate showing the optimum energy-throughput range.

of 500ms of packets of 128 bits each. At each bitrate and power level, we ran 3 experimental trials, and we experimented with 10 bitrates in total (50kbps, 100kbps, 250kbps, 500kbps, 1Mbps, 2Mbps, 2.5Mbps, 3Mbps, 4Mbps, 5Mbps) and three transmit power levels to correspond to different in-tissue conditions (19dBm, 16dBm, 14dBm). We computed the BER for each bitrate and transmit power as the fraction of incorrectly decoded bits to the total bits transmitted. Recall that the backscatter encoder uses FM0, and our external reader uses a maximum likelihood decoder.

Fig. 3-26 plots the BER as a function of backscatter bitrate for each of the three power levels (purple for 19dBm, red for 16dBm, and green for 14dBm). The figure shows that as the bitrate increases, the BER also increases. This is because higher bitrate requires larger bandwidth, thus increasing the received noise. This figure also shows that if the transmit power increases, the BER decreases; this is also expected because a higher transmit power results in higher backscatter (reflected) SNR, resulting in better decoding ability. This demonstrates the need to adapt the channel not only to the harvested energy as described in section 3.5 but also to the SNR.

(c) BER-SNR Curves. Recall that the external receiver is implemented as a maximum likelihood detector. Next, we evaluated the receiver's ability to correctly decode backscatter packets transmitted on the uplink. This is typically assessed by plotting the BER-SNR curve. Fig. 3-27 plots the BER-SNR of the receiver from the same experimental trials described above. It shows that the BER decreases with increased SNR following the expected theoretical trend.

(d) Assessing Adaptation. Our final evaluation focuses on understanding the trade-off between availability and throughput and how μmedIC's bitrate adaptation algorithm (described in section 3.5) allows adapting the bitrate without sacrificing availability. To this end, we compare the performance of three different schemes, all in time-varying channels. The first uses a fixed low backscatter rate of around 625kbps; the second uses a fixed high rate of around 10Mbps; the third adapts its rate according

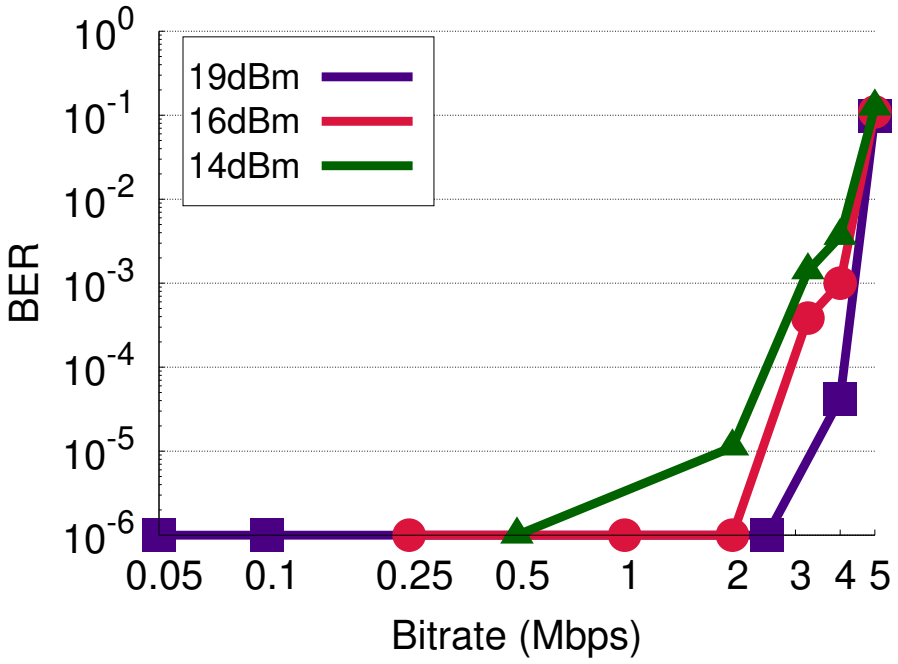


Figure 3-26: **BER vs Bitrate.** The figure plots the bit error rate as a function of bitrate at different power levels: 14dBm (green), 16dBm (red), and 19dBm (purple).

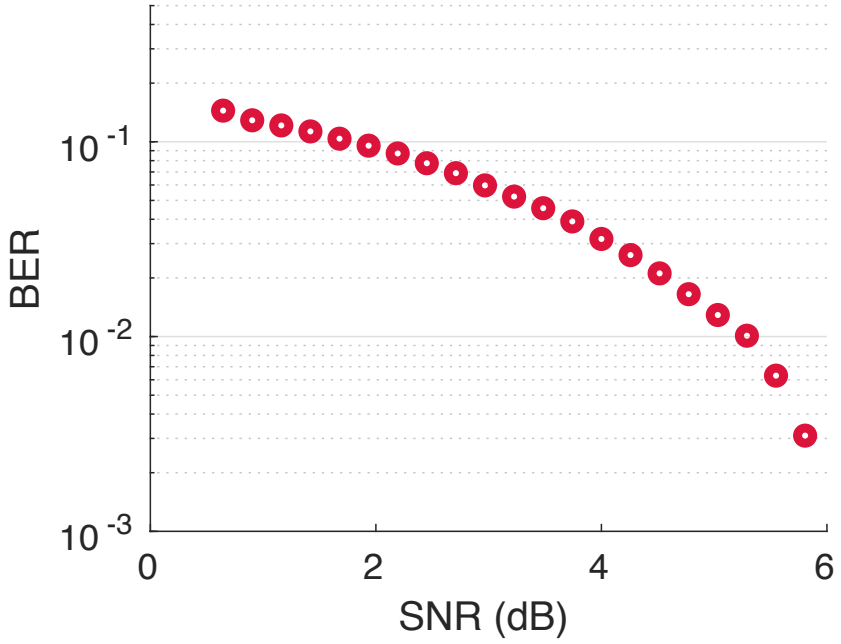
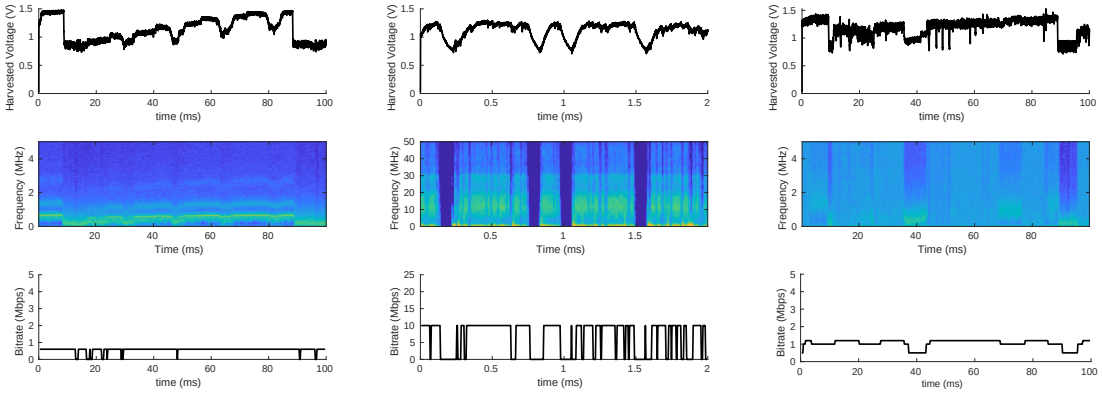


Figure 3-27: **BER vs SNR.** This figure plots the bit error rate against different SNR levels showing that it follows the expected theoretical trend.



(a) Fixed Low-Rate Configuration (b) Fixed High-Rate Configuration (c) Adaptive-Rate Configuration

Figure 3-28: **μmedIC across Fixed and Adaptive Schemes.** The figure plots μmedIC's performance across different configurations: (a) fixed low-rate, (b) fixed high-rate, and (c) adaptive rate. The top row plots the harvested DC voltage over time. The middle row plots the oscillator frequency as a spectrogram heatmap over time, where yellow indicates high-intensity and blue indicates low-intensity. The bottom row plots the effective bitrate across time.

to the energy stored in the harvester's storage capacitor as per the algorithm described in 3.5.

Fig. 3-28 shows the three different schemes in time-varying channels. The top row plots the harvested voltage versus time for each of the three schemes. The middle row plots the spectrogram (representing the backscatter frequency)which is shown as a heatmap where high power at a specific frequency is indicated by red or yellow and where blue indicates the absence of the corresponding frequency. And finally, the bottom row shows the instantaneous bitrate inferred from the spectrogram. Figs. 3-28(a), (b), and (c) represent the low-bitrate, high-bitrate, and adaptive bitrate schemes respectively.

We make the following remarks:

- For the low-bitrate scheme, throughput remains constant at around 625kbps without taking advantage of higher available power at better channels. This can be seen both from the spectrogram and the instantaneous bitrate. The oscillator rarely dies in this scheme due the low power consumption and conservative nature.

- When the node fixes its rate to the high mode regardless of the available power, it suffers from frequent power downs during transmission as illustrated in the spectrogram of Fig. 3-28(b).

- Finally, the adaptive scheme shown in Fig. 3-28(c) can smoothly adapt its bitrate from one packet to the other according to the received power variations.

To better understand the benefits of rate adaptation, consider a scenario where the sensor transmits packets of 5,000bits. In the fixed bitrate case of 500kbps, the packet length would be 10ms, and the overall goodput is around 350kbps (Since packet transmission restarts whenever the sensor dies, 7 out of 10 packets will be delivered within the 100ms interval). In the fixed bitrate of 10Mbps, the packet length would be 5ms, and the overall goodput is 0kbps (none of the packets are delivered since the sensor keeps dying before finishing the transmission). Finally, for the bitrate adaptation case, the average bitrate is above 1Mbps, thus exceeding both the low and high bitrate scenarios. Note that we experimented with other packet sizes as well, and the throughput improvement from bitrate adaptation depends on the packet size and SNR variations.

To gain more insight into the tradeoff between availability and throughput, we collected measurements across three schemes, similar to the ones described above: a fixed low rate of 750kbps, a fixed high rate of 12Mbps, and an adaptive rate scheme capable of varying between the two. We ran around 30 experimental trials in total covering low-power, high-power, and varying-power environmental setups. In order to ensure the nodes experienced a time-varying channel in the latter, we programmed our downlink transmitter to quickly vary its transmit power by a factor of 2 each 20 ms. In each experimental trial, we estimated the node failure probability as our availability metric. The empirical probability was computed as the ratio of period of time the node fails (due to running out of power) to the full duration of the transmission.

Fig. 3-29 shows the results of this experiment by plotting the node failure probability

across the different schemes and setups, where Fig. 3-29(a), (b), and (c) represent the low-power, high-power, and varying-power setups respectively. The bar graphs correspond to the median failure probability and the error bars show the standard deviation. We make the following remarks:

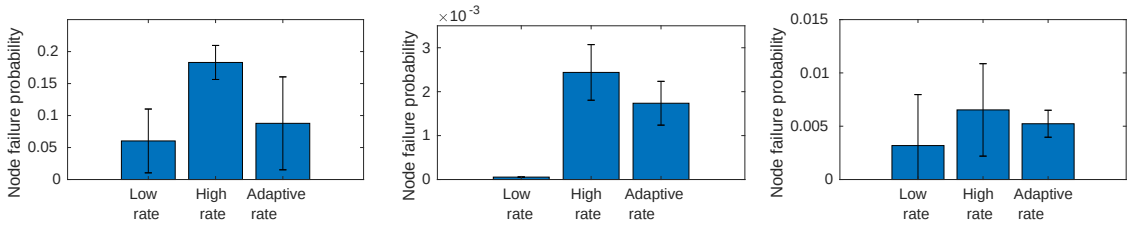
- μmedIC's low-rate scheme provides the highest availability. Specifically, even under the lowest-power mode, it's failure probability remains below 0.06 (i.e. 6%), and it drops further to 0.0055 at higher power channels. This is expected since the low-rate scheme consumes the lowest power (as per Fig. 3-25).

- The high-rate scheme suffers from a node failure probability of 0.2 in the low-power regime. This demonstrates that high-rate is likely to be unsuitable for applications that require always-on availability for in-body sensing (and communication).

- In the high-power setup (Fig. 3-29(b)), almost all modes have high availability, with even the high-rate mode having a failure probability lower than 0.0003. This suggests that in high-power settings, there is little to be gained from using the low-rate scheme.

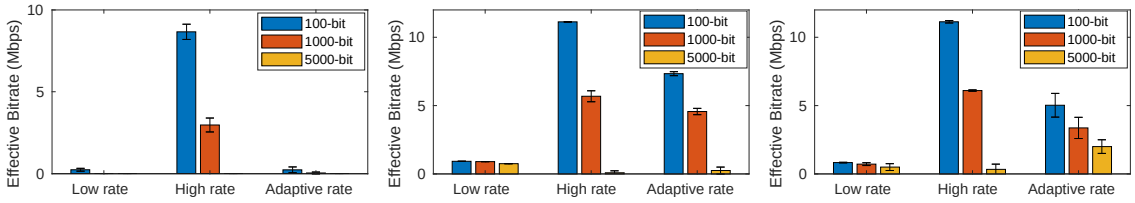
- Finally, μmedIC's adaptive scheme offers a middle ground between low-rate and high-rate. In principle, it is possible to make the adaptive rate more conservative or aggressive by adjusting the adaptation thresholds, which would result in performance that is closer to the low-rate or high-rate schemes respectively.

So far, we have demonstrated that μmedIC's ability to choose and/or adapt its bitrate enables it to adapt for availability. Next, we would like to understand how these different schemes compare in terms of effective throughput. To do this, we used the same experimental trials described above and performed trace-driven simulations to measure effective bitrate. We also compared different packet sizes to understand



(a) Low-Power Settings (b) High-Power Settings (c) Varying-Power Settings

Figure 3-29: **Availability vs Configuration.** The figure plots the median failure probability of a node across different configurations in (a) low-power, (b) high-power, and (c) varying-power settings. The error bars represent the standard deviations.



(a) Low-Power Settings (b) High-Power Settings (c) Varying-Power Settings

Figure 3-30: **Throughput vs Configuration.** The figure plots the median effective bitrate across configurations in (a) low-power, (b) high-power, and (c) varying-power setting. The error bars represent the standard deviations.

the impact of packet size on throughput. The effective bitrate is computed as the number of total packets successfully transmitted (before failing) multiplied by the number of payload bits per packet and divided by the entire transmit duration. Note that if a node fails in the middle of a packet transmission, we consider the entire packet to be lost, thus emulating practical flows.

Fig. 3-30 plots the effective bitrate for each chip configuration across the different schemes and setups, where Fig. 3-30(a), (b), and (c) represent the low-power, high-power, and varying-power setups respectively. The figure also shows the effective bitrate for different packet sizes, 100-bit packet (shown in blue), 1000-bit packet (shown in orange), and 5000-bit packet (shown in yellow). The bar plot represents the median rate while the error bar represents the standard deviation. We make the following remarks:

- The high-rate scheme provides the highest throughput (effective bitrate) across

almost all setups, even the low-power setup. In particular, for the 100-bit packet size, it achieves bitrates between 8.5Mbps and 11.5Mbps across the different setups. While this may be counter-intuitive (given that the high-rate has the lowest availability as per Fig. 3-29), it is able to transmit more bits within the same duration of time due to its higher bitrate. This shows that if the goal is to achieve the highest throughput (rather than the highest availability), then it is more desirable to configure μmedIC to its high-rate mode.

- The 100-bit packet size (blue) outperforms all other schemes, despite that it suffers from more overhead since it has the same header size as the other schemes but smaller payload. This is because the chip is prone to suffer from node failure; thus, it is more desirable to get a full packet across than it is to aim for transmitting a longer packet with less overhead.

- Interestingly, the adaptive rate mode performs the best for largest packet size (5000-bits) in time-varying channel, i.e., in Fig. 3-30(c). This is because it can transmit at higher bitrates than the low-rate and does not fail as frequently as the high-rate configuration.

These results demonstrate that μmedIC's ability to switch between different configurations (whether fixed or adaptive bitrate) allows reconfiguring it to the application requirements. For instance, a streaming application may require continuous transmission, and thus favor availability over throughput (i.e., low-rate). Other applications may require higher throughput (e.g., taking one snapshot image and transmitting it quickly, with little buffering), and such applications may choose either high rate or aggressive rate adaptation. More generally, these results demonstrates the value of μmedIC's programmable throughput to serve different application requirements.

3.9 Conclusion

This chapter presents μmedIC, a self-reconfiguring fully-integrated wireless platform for batteryless in-body sensors. Our platform employs programmable structures in its antenna, harvesting circuits, and logic. The design is implemented on an IC and tested across tissues to demonstrate its ability to adapt its energy harvesting and backscatter throughput. Looking ahead, this technology paves way for a new generation for networked micro-implants capable of adapting to complex and time-varying in-body conditions.

Chapter 4

Wireless Secure Pressure Sensing Implant

The previous chapter focused on the design of a reconfigurable RF front-end with the transmitter backscattering external bits or a fixed sequence. This chapter builds on the previous chapters and presents the integration of the reconfigurable RF front-end with a pressure-sensing analog front-end and a security engine for data privacy and transmitter authenticity.

4.1 Introduction

In-body gastrointestinal (GI) pressure sensing systems can provide means for long-term monitoring of the GI tract motility. Measuring the in-body GI tract motility captures the changes in the flow of the gastric fluids which aids in understanding digestive disorders as well as obesity development.

Building micro-implanted systems for GI pressure sensing requires satisfying competing design requirements. These systems need to be *batteryless, wireless, available, small*, and *secure*. Independence of batteries eliminates the need for surgical replacement, allows ultra-long term operation, and enables miniature, fully-integrated form

factors. Wireless communication is necessary for tasks that involve continuous monitoring, capturing transient anomalies, remote operation, or closed-loop control. Such communication also needs to be always-available to allow for immediate intervention (e.g., drug release). Security is essential in protecting the privacy of the patient's data in addition to authenticating the base station reader. Finally, the need to operate in different tissues is particularly important for mobile micro-implants which experience a variety of in-body environments as they travel through the human body.

Despite important steps toward enabling GI health monitoring implants, none of today's systems can satisfy all these requirements. The advancements in flexible sensors design have witnessed the exploit of ultrasound conformal sensing materials such as lead-zirconate-titanate pressure sensors for gastrointestinal motility monitoring [77,78]. However, these systems require long wires to extract their sensed data. Others have demonstrated general in-body pressure sensing systems with batteryless ultrasonic data and power links [79], but in contrast to wireless RF operation, ultrasonic links provide a limited range of operation. While on-chip security accelerators have been demonstrated in the literature [80,105], a batteryless secure implantable system for GI pressure sensing is yet to be presented.

In this chapter, we demonstrate for the first time the potential to build a wireless batteryless pressure sensor for GI-tract motility sensing. In principle, one could build a fully-integrated wireless system that combines a variety of existing components, e.g., juxtaposing a wireless communication module with an analog front-end (ADC), an energy harvesting unit, and a security engine. However, such a simple integration approach would not be ideal for two main reasons. First, each additional component would incur additional energy consumption and area. Second, it would require making undesirable trade-offs between the functionality, energy-efficiency, and latency. For example, existing designs for energy-efficient high-sensitivity analog front-ends for pressure sensing typically have high-latency, which in turns results in unnecessary

energy consumption. In contrast, we would like to achieve high sensitivity in an energy-efficiency, compact, and low-latency design. Building such system requires multiple key innovations along two fronts:

1. **Over-the-Air Closed-Loop Wireless Programming:**

   PZ-Sense's first innovation is to leverage the asymmetric nature of our end-to-end design in order to mitigate the trade-off between functionality, energy-efficiency, and latency. In particular, rather than treating the analog front-end as separate from the communication protocol, it leverages the protocol itself to make the front-end more efficient; this can be achieved by offloading some of the computations to an external reader that memorizes the earlier sensing state and shares it with the sensor upon powering it up. This same idea can also be extended to enable high-efficiency harvesting and rate adaptation. In particular, rather than requiring the IC to do a costly search for the ideal parameters to tune to the surrounding tissues (as discussed in Chapter 3), we enable the reader to memorize and downlink the ideal configuration via over-the-air programming. These techniques are described in detail in sections 4.3 and 4.4.3.

2. **A Fully Integrated Security-Sensing-Communication Stack:**

   PZ-Sense second innovation demonstrates that rather than treating each layer separately, we can share some of the circuit components to lower the power consumption and the active chip area. In particular, we illustrate how the ADC can be used as a a front-end pressure sampler as well as reused as a TRNG for AES-GCM security engine. Similarly, we amortize the latency of the programmability by designing a logic pipeline that can perform full circuit reprogrammability using a single packet. These techniques are described in detail in Chapter 5.

This chapter focuses on the design of the sensor front end as well as the closed-loop

over-the-air programming while the next chapter describes the security engine and the ADC-reuse.

4.2 System Overview

We designed, fabricated, and tested our system, outlined in Fig. 4-1, in a TSMC 65nm 2mm×1mm CMOS chip[1]. A Lead-Zirconate-Titanate (PZT) pressure sensor is to be fabricated and interfaced with the chip and the whole system is integrated on a flexible PCB and matched with a microstrip loop antenna for power delivery and data communication.

The proposed system is composed of four subsystems: energy harvesting, transmit/receive chains, analog front-end interface, and a security engine. The energy harvesting and power management system (EH & PMU) which consists of a 6-stage differential cross-connected rectifier followed by a voltage limiter and a low-dropout regulator (LDO). The receiver chain ac couples the envelope of the RF signal into a baseband amplifier followed by a integrate-and-dump decoder for the Pulse Interval Encoded (PIE) input bits while the transmitter chain encodes its bits into FM0 encoding and transmits via backscatter through a digitally controlled ring oscillator (DCO). The analog front end (AFE), done in collaboration with Unsoo Ha, is composed of a low noise amplifier (LNA), a programmable gain amplifier (PGA) and a 10-bit SAR ADC. Fig. 4-2 shows the schematic of the AFE where, initially, a closed loop is formed using an accumulating logic for the DC cancellation of the sensor's nominal measurement and extracting the small signal fluctuations. The security engine, done in collaboration with Utsav Banerjee, implements an advanced encryption standard in Galois/Counter mode (AES-128-GCM) for decryption, authentication, and encryption [80]. Additionally, it utilizes an on-chip initial vector generation using a true

[1]The sensor front end is designed in collaboration with Unsoo Ha while the custom strain sensor is in collaboration with Prof. Canan Dagdeviren.

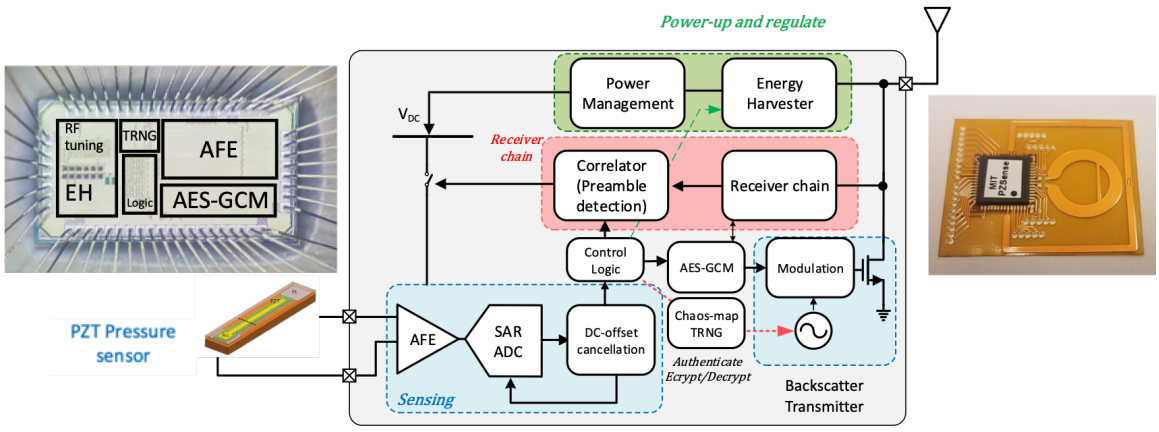


Figure 4-1: **PZSense.** Block diagram of the Pressure sensing node while showing the diephoto and board assembly.

random number generation (TRNG) via a discrete time chaos map in the form of a closed loop residue amplifying multiplying DAC (MDAC) in conjunction with the SAR ADC.

4.3 Circuit Description

In this section, we describe the circuit schematics of the different building blocks of the proposed pressure sensing node. First, we highlight the pressure sensor front-end circuits, then, we talk about the rest of the circuits in our system.

Sensor Front End

The sensor front end is composed of a custom designed amplification and filtering front-end which interfaces directly with the custom pressure sensor. The schematic for such front-end is illustrated in Fig. 4-2 where a low noise amplifier (LNA) performs the initial strain-induced charge amplification and filtering then a programmable gain amplifier (PGA) provides a programmable second level of amplification. The full range output is then quantized by a 10-bit SAR ADC to produce the digital sensor data to the encryption block and later to the backscatter switches for data transmission back

to the reader.

For the minute fluctuations of the strain sensor for pressure sensing, the gain of the front-end amplifier chain is quite high. For instance, the LNA gain can be programmed to be either 50× or 10× while the PGA gain has a 3-bit programmable range from 10× up to 100×. With a maximum gain of $5000V/V$ ($74dB$), any small DC offset ($\geq 500\mu V$) in the custom sensor, the LNA, or the PGA propagates from one stage to the other to saturate the input dynamic range of the ADC which operates at a supply voltage of almost $V_{DD,LDO} = 0.5V$. Therefore, in order to mitigate this issue, we incorporate an offset cancellation loop as depicted in Fig. 4-2. The front-end amplifiers along with the ADC are tied in a feedback loop where a digital accumulator is used to tune the offsets of the amplifiers till the system converges to an offset-free steady state.

The front-end operational transconductance amplifiers (OTA) are designed as two-stage OTAs with a fully differential folded cascode first stage followed by a common

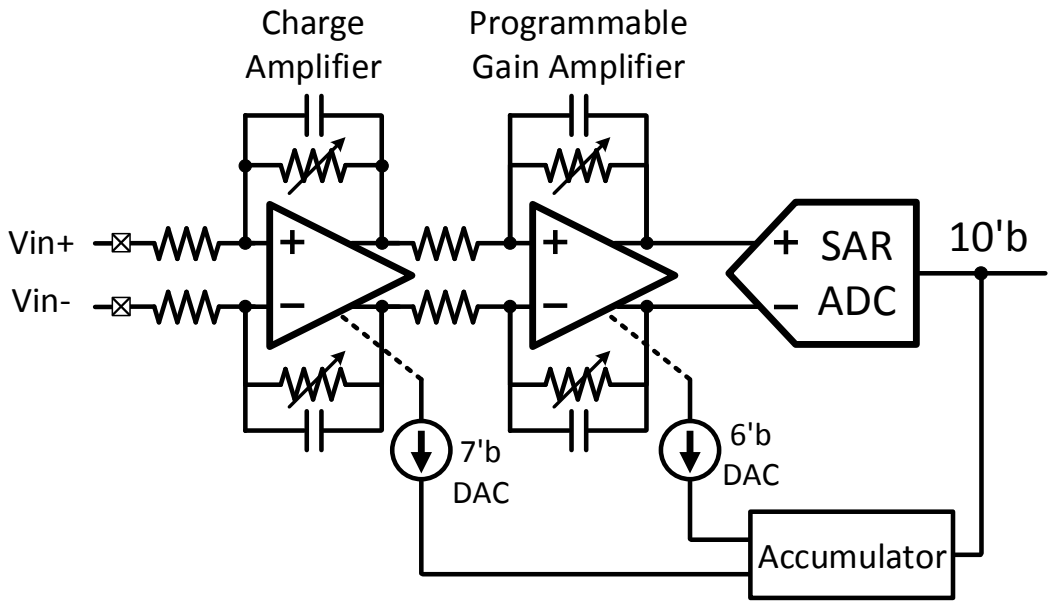


Figure 4-2: **Analog Front End.** Schematic diagram of the sensor front end showing the LNA, PGA, and DC cancellation loop.

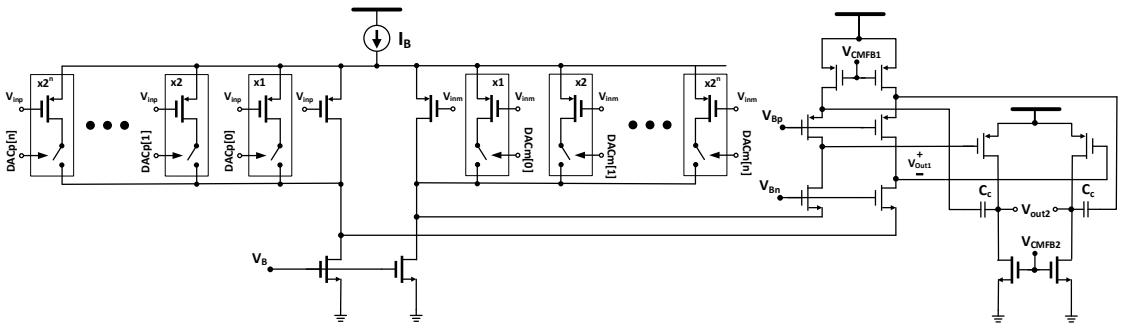


Figure 4-3: **Charge amplifier OTA.** Schematic diagram of the operational transconductance amplifier used in the LNA showing the offset cancellation switches in the input differential pair.

source differential second stage. Analyzing the sources of offset in the OTA, we can conclude that the input referred offset is dominated by the input differential pair, and is given by:

$$v_{OS,in}^2 = v_{OS,diff}^2 + v_{OS,bias}^2 \cdot \left(\frac{g_{m,bias}}{g_{m,diff}}\right)^2 \tag{4.1}$$

$$v_{OS,in}^2 \simeq v_{OS,diff}^2 = \frac{A_v^2}{WL} \tag{4.2}$$

where $v_{OS,diff}$ and $g_{m,diff}$ are the input differential pair offset and transconductance respectively while $v_{OS,bias}$ and $g_{m,bias}$ are the current mirror offset and transconductance respectively, A_v is a proportionality constant for the V_{th} variations while W and L are the channel width and length respectively.

Hence, the input differential pair of the LNA's (and PGA's) OTA employs a 6-bit (5-bit) binary weighted programmable pairs in order to effectively increase the width of the input pair and reduce the input referred offset with the closed loop feedback. The full schematic of the LNA's OTA is shown in Fig. 4-3 showing the amplifier circuit and the offset cancellation switches while excluding the Common-mode feedback (CMFB) circuits used to define the common mode DC voltages for the OTA stages.

After the offset cancellation loop settles, it is turned off and the sensor data are then quantized using a 10-bit SAR ADC, shown in Fig. 4-4 where it utilizes

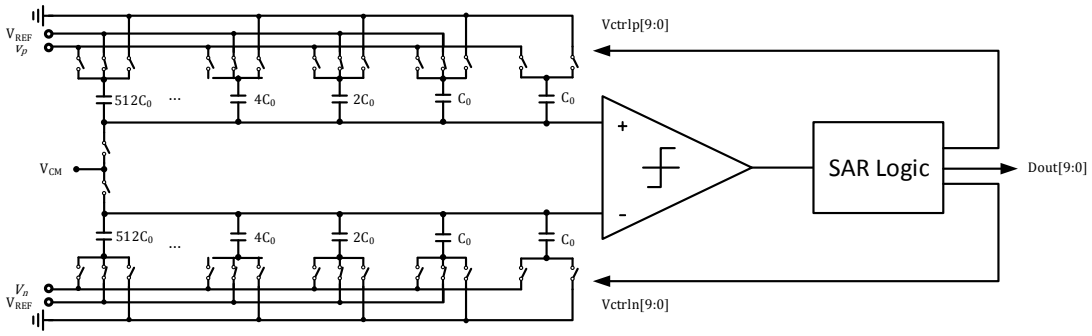


Figure 4-4: **SAR ADC.** Schematic diagram of the 10-bit SAR ADC used in the sensor front end.

a switched-capacitor architecture to sample the input, compare with the reference voltage in a *binary search* fashion in order to settle on the final 10-bit output samples.

The system closes the loop with the base station by backscattering its final accumulator state as well as final gain parameters, then the base station can set the gains and initial state of the node through the downlink command providing a faster settling time and an adequate gain for the highest dynamic range.

Security Engine and TRNG

In the downlink path, the security engine provides two main functions: a) to authenticate the transmitter node and b) to decrypt the incoming downlink command. Similarly, on the uplink, it encrypts the buffered sensor samples and generates an authentication tag using the shared key for the reader to authenticate its packets. For this purpose, a highly parallelized architecture where a 128-bit datapath is implemented with parallel non-linear blocks to achieve better energy efficiency and faster operation even at the expense of larger silicon area [80].

Since AES-GCM is a counter-mode encryption, it behaves like a stream, and hence, requires a different initialization vector (IV) for each stream of data to ensure security. To provide such IV, an analog true random number generator (TRNG) is proposed through the use of discrete time switched capacitor chaos maps. Additionally, we

reuse the sampling ADC to quantize the discrete random output of the TRNG at a power overhead of only 2% compared to building a dedicated PRNG circuit.

Different switched-capacitor circuits have been proposed as a means of implementing discrete time chaos maps. The work in [81] utilizes a 1.5-bit pipeline ADC stage to generate a stream of TRNG bits by feeding the residue back to the input of the pipeline stage and XORing the 2-bit output of the sub-ADC in the first stage of the pipeline architecture. Similarly, the proposed system in [82] uses a subranging ADC to generate a higher bitrate random stream through residue feedback based on a random initial state. Additionally, ring-oscillator based TRNG utilizes the timing jitter to generate random bits such as the designs in [83] and [84].

A conventional pipeline ADC stage is shown in Fig. 4-6 a) where a multiplying DAC (MDAC) works as a subtracting DAC as well as a residue amplifier. Such MDAC can be adapted into a chaos map circuit by closing the loop between the residue and the input as shown in Fig. 4-6 b). In this case, the output is given by:

$$v_{out}[n] = \left(\left(1 + \frac{C_1}{C_2}\right) \cdot v_{out}[n-1] + v_n\right) \mod V_{REF} \tag{4.3}$$

where v_n is the output integrated noise sample and V_{REF} is the stage's reference voltage. This circuit is basically equivalent to a dyadic transformation (or a chaotic logistic map) which diverges to span all states as long as it has a non-zero initial condition. This is illustrated by the bifurcation plot in Fig. 4-5 where all the encountered states are plotted against the gain parameter showing that for a residue amplification gain of 2×, the circuit becomes chaotic covering all states from $-V_{REF}/2$ to $V_{REF}/2$.

Therefore, we implement the MDAC-based TRNG and reuse the sensor front-end SAR ADC to sample the analog random output and feed it to the security engine. The TRNG OTA is the main source of noise in this TRNG and guarantees a non-zero initial state of operation. It is designed a two-stage Miller-compensated operational

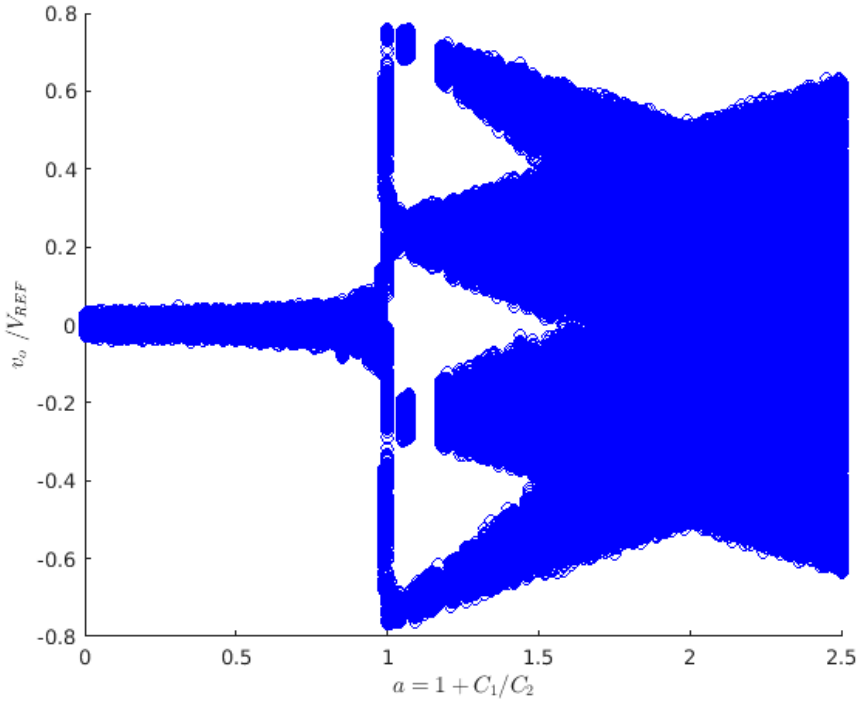


Figure 4-5: **Chaos map Bifurcation.** The figure plots the values approached by the system as a function of the gain parameter for a non-zero initial condition.

amplifier with a resistive CMFB circuit as shown in Fig. 4-7. The input referred noise of such OTA is analyzed to be:

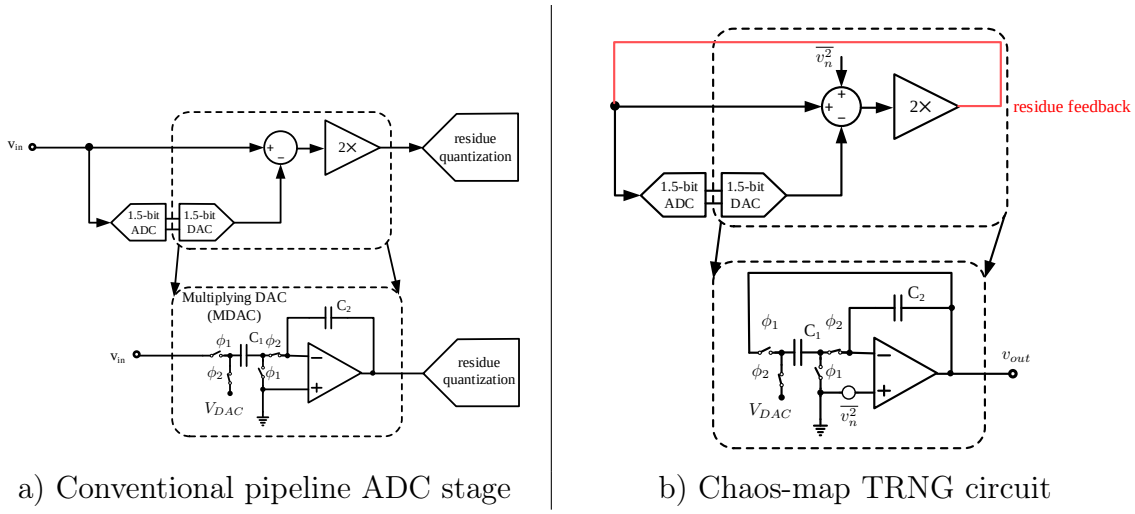
$$\overline{v_{n,in}^2} = 2 \times \left(\overline{v_1^2} + \overline{v_3^2} \cdot \left(\frac{g_{m3}}{g_{m1}} \right)^2 + \overline{v_5^2} \cdot \left(\frac{1}{g_{m1} R_{o1}} \right)^2 + \overline{v_7^2} \cdot \left(\frac{g_{m7}}{g_{m1} R_{o1} g_{m5}} \right)^2 \right) \quad (4.4)$$

$$\overline{v_i^2} = \frac{2nkT}{g_{mi}} \qquad \forall\ i \in [1, 8] \quad (4.5)$$

where g_{mi} is the i^{th} transistor transconductance while $\overline{v_i^2}$ is the input referred mean squared voltage noise of each transistor, assuming that the even transistors are matched with the odd ones. The noise in the subthreshold region is defined by the absolute temperature T, Boltzmann's constant k, and the subthreshold ideality factor n.

With a gain-bandwidth product of the two stage opamp given by:

$$\omega_c = A_0 \cdot \omega_p = \frac{g_{m1}}{C_c} \quad (4.6)$$



a) Conventional pipeline ADC stage

b) Chaos-map TRNG circuit

Figure 4-6: **TRNG.** The figure shows the pipeline ADC stage and the proposed adaptation for a discrete-time chaos-map circuit.

where A_0 is the DC gain of the OTA, ω_p is the pole frequency, and C_c is the Miller compensation capacitor, the closed loop noise bandwidth is given by:

$$BW = \beta \cdot \omega_c = \frac{C_2}{C_1 + C_2} \cdot \frac{g_{m1}}{C_c} \tag{4.7}$$

where C_1 and C_2 are the sampling and feedback capacitors respectively. Hence, the total integrated noise added to each sample at the output of the amplifier becomes:

$$\overline{v_{o,int}^2} = \int_0^\infty \overline{v_{n,in}^2} \cdot \left(\frac{A_0}{1 + A_0\beta}\right)^2 df \simeq \overline{v_{n,in}^2} \cdot \left(1 + \frac{C_2}{C_1}\right)^2 \cdot \frac{BW}{4} \tag{4.8}$$

$$= \overline{v_{n,in}^2} \cdot \frac{g_{m1}}{\beta C_c} \simeq 2 \times \frac{2nkT}{\beta C_c} \tag{4.9}$$

where the first stage differential pair shot noise is the most dominant factor.

The bandwidth of the OTA and its transconductance are chosen to guarantee that the TRNG settles within one clock cycle while providing the noise to be accumulated as the initial seed of the TRNG.

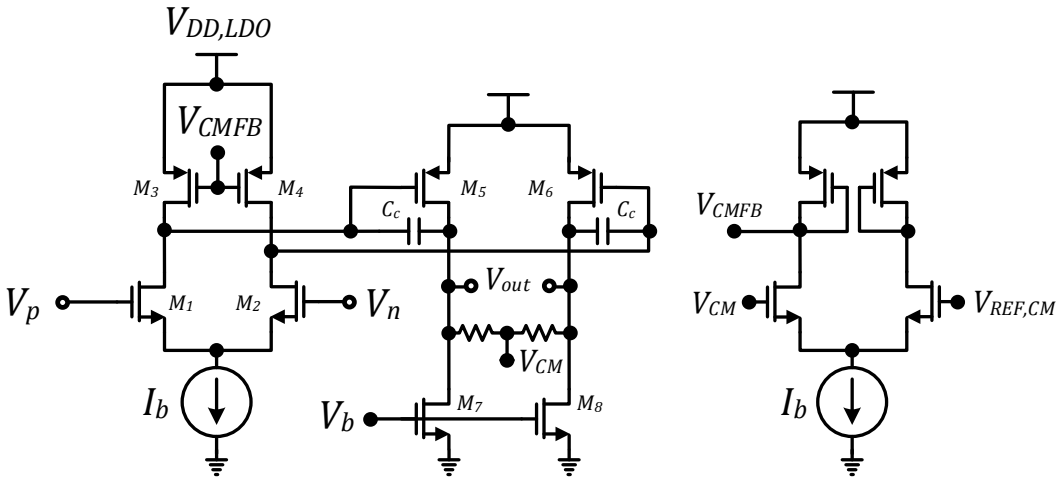


Figure 4-7: **TRNG OTA.** Schematic diagram of the 2-stage operational transconductance amplifier used in the TRNG circuit.

4.3.1 RF energy harvesting and communication

- **Harvesting and Power Management Path:**

  The energy harvesting chain adopts an N-stage rectifier design similar to the one described in Section 3.6 with a focus on reducing the parasitic capacitances and resistances in the layout of the rectifier as well as the tunable capacitor banks. Additionally, the LDO is re-optimized for the newer power consumption with the security engine as well as the sensor front-end circuits.

- **Antenna Design:**

  The proposed system employs a loop antenna with a coupled outer loop for a reconfigurable resonance frequency, similar to the design of μmedIC. In this part, however, we focused on designing a higher-Q inductive antenna to match the more optimum rectifier layout and achieve an overall better sensitivity.

- **Communication Circuits:**

  This SoC also incorporates an envelope detector receiver with a PIE decoder for the downlink packet similar to the design explained previously in the μmedIC

chip in Section 3.6. And similarly, the transmitter utilizes backscatter to transmit FM0 encoded signals back to the reader.

4.4 Measurement Results

This section shows the measured waveforms for different operations of the chip illustrating how the chip goes from energy harvesting, to sensing, encryption, and communication.

4.4.1 Measurement Setup

In order to test the SoC in a wireless setup, a custom RF source is implemented on an RF signal generator [85] and then hooked up to a transmitting antenna [74]. Then the chip testing board is connected to an Opal Kelly FPGA level shifting and extracting the outputs to be saved on internal registers, and also, to send any manual configuration bits for testing and debugging purposes.

4.4.2 Energy Harvesting and Power Management

The chip starts by the N-stage rectifier which harvests the RF energy from a reader node through the reconfigurable loop antenna and stores it over a storage capacitor. Then, the LDO generates a regulated supply voltage of around $0.55V$ for the rest of the blocks while a delayed Power on Reset (PoR) signal is generated to reset all the internal flip flops and initialize the state machine as shown in Fig. 4-8.

4.4.3 Downlink Operation

After the reader powers up the chip with a continuous wave (CW) RF signal, it switches to an On-off Keying (OOK) signal to transmit a downlink command encoded with PIE scheme. Fig. 4-9 illustrates how the receiver employs an envelope detector followed

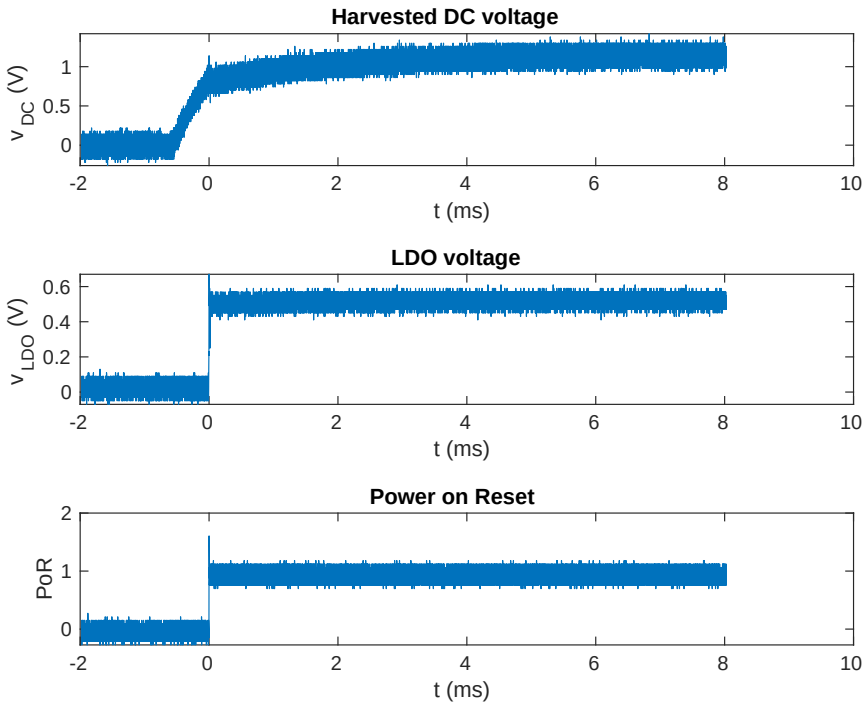


Figure 4-8: **Energy Harvesting Measurement.** Measured transient waveforms of the harvested DC voltage, the LDO output, and PoR during a continuous RF powering up transmission.

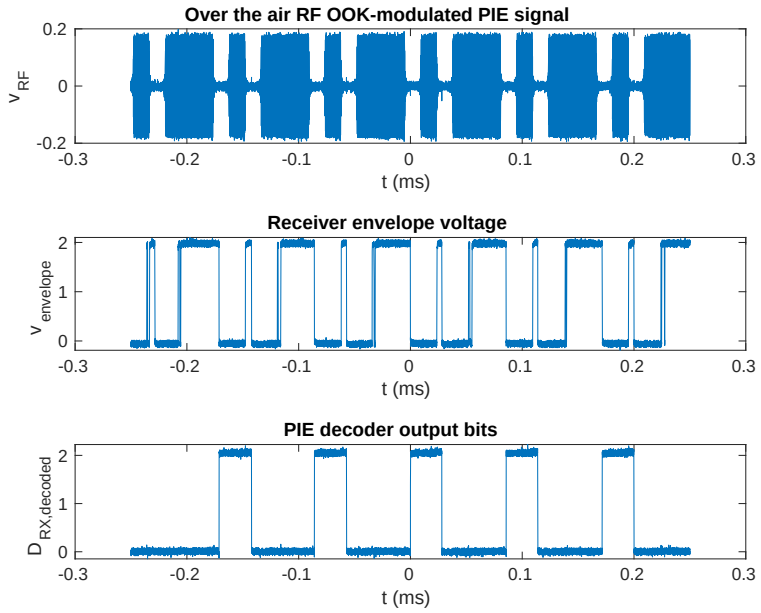


Figure 4-9: **Receiver Downlink Measurement.** Measured transient waveforms of the receiver are plotted for the preamble of a packet consisting of a stream of '1010...' bits. The figure shows the RF signal along with the output of the envelop detector and the PIE decoder.

by an integrate-and-dump decoder to extract the output bits from the incoming modulated RF signal.

The decoded bits then are fed into a correlator which compares the input bits with a predetermined preamble to determine the beginning of the packet. Once the correlator triggers, the the full packet is then loaded into the security engine which authenticates the transmitter through comparing with the authentication tag and then, decrypts the full packet using the IV and the pre-shared key.

If the correlation result is below the preamble's threshold or the authentication tag gives a '0', then the chip returns to the charge and receive state. Otherwise, it extracts the downlink command and branches into a "Reconfigure" state where it reprograms the input matching for different surrounding tissues, tunes the antenna resonance, or set the initial values for the offset cancellation loop in the sensor front end according to the incoming downlink packet. Fig. 4-10 shows the measured transient waveforms

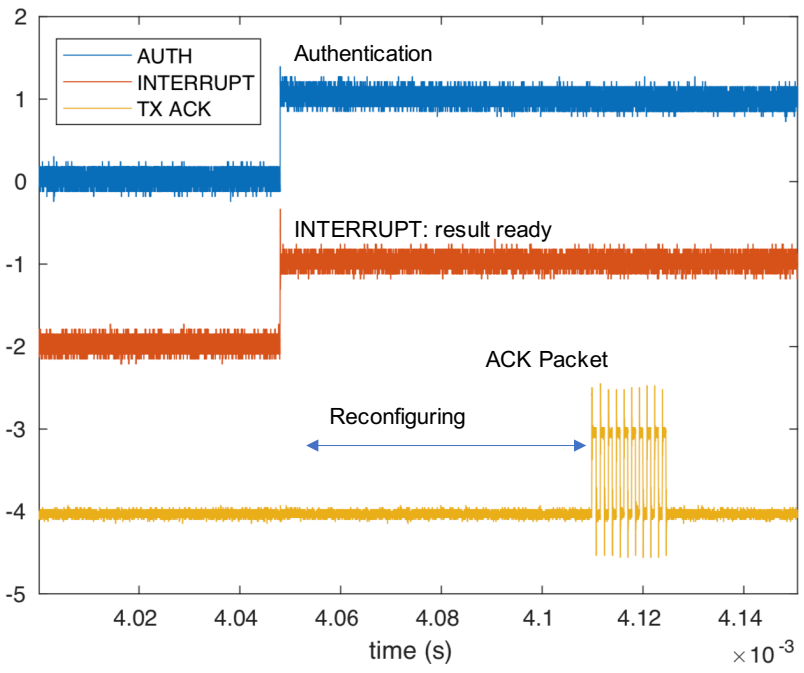


Figure 4-10: **"Reconfigure" command operation.** Measured transient waveforms of the authentication flag, interrupt flag, and the transmitter bits for a "Reconfigure" packet

for a "Reconfigure" packet where the chip backscatters an Acknowledge (ACK) packet back to the reader once it finishes reconfiguring its internal blocks.

4.4.4 Uplink Operation

For the "Sense" command, the SoC branches into the pressure-sensing states enabling the sensor-front end to continuously sample the sensor's output. The transient operation of the uplink path is plotted in Fig. 4-11 where the *interrupt* signals the end of the authentication and decryption operation. Then, the authentication flag triggers the front-end where the ADC bits start plotting the sampled sensor output. Afterwards, the security engine buffers the input samples and divides the encrypted packets into a burst of packets to be transmitted along with the node ID, IV, and the generated authentication tag.

A zoomed-in view of the measured uplink packet bits is plotted in Fig. 4-12 where

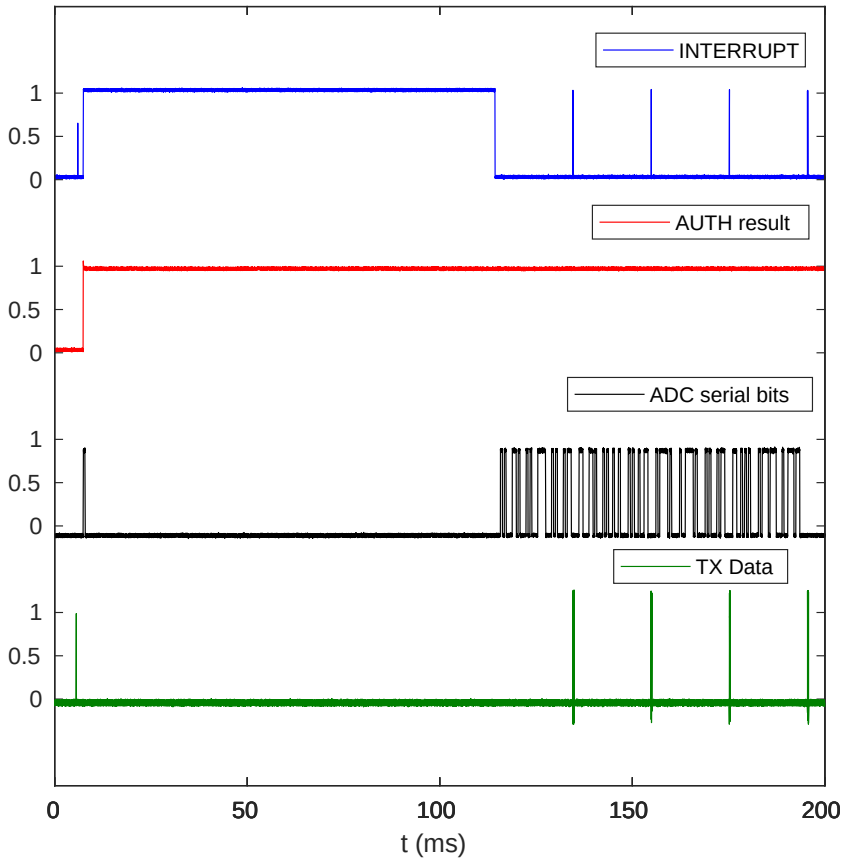


Figure 4-11: **"Sense" command operation.** Measured transient waveforms of the interrupt flag, the authentication result, the ADC serial output bits, and the transmitted bits in the burst-mode sensing operation.

the packet is divided into: a) a 32-bit node ID to identify the node, b) a 96-bit IV used to decrypt and authenticate, c) a variable-size encrypted payload, and d) a 128-bit authentication tag.

The buffered bursts of packets coming out of the security engine are then fed to an FM0-encoder which passes the encoded bits to the backscattering switches to produce transmit the data back to the reader. A portion of the packet is illustrated in Fig. 4-13 where the wireless backscattered RF signal is plotted along with an ideally-generated FM0 signal for the beginning of the packet containing the node ID set as 0xAAA12345 at a datarate of almost 1Mbps.

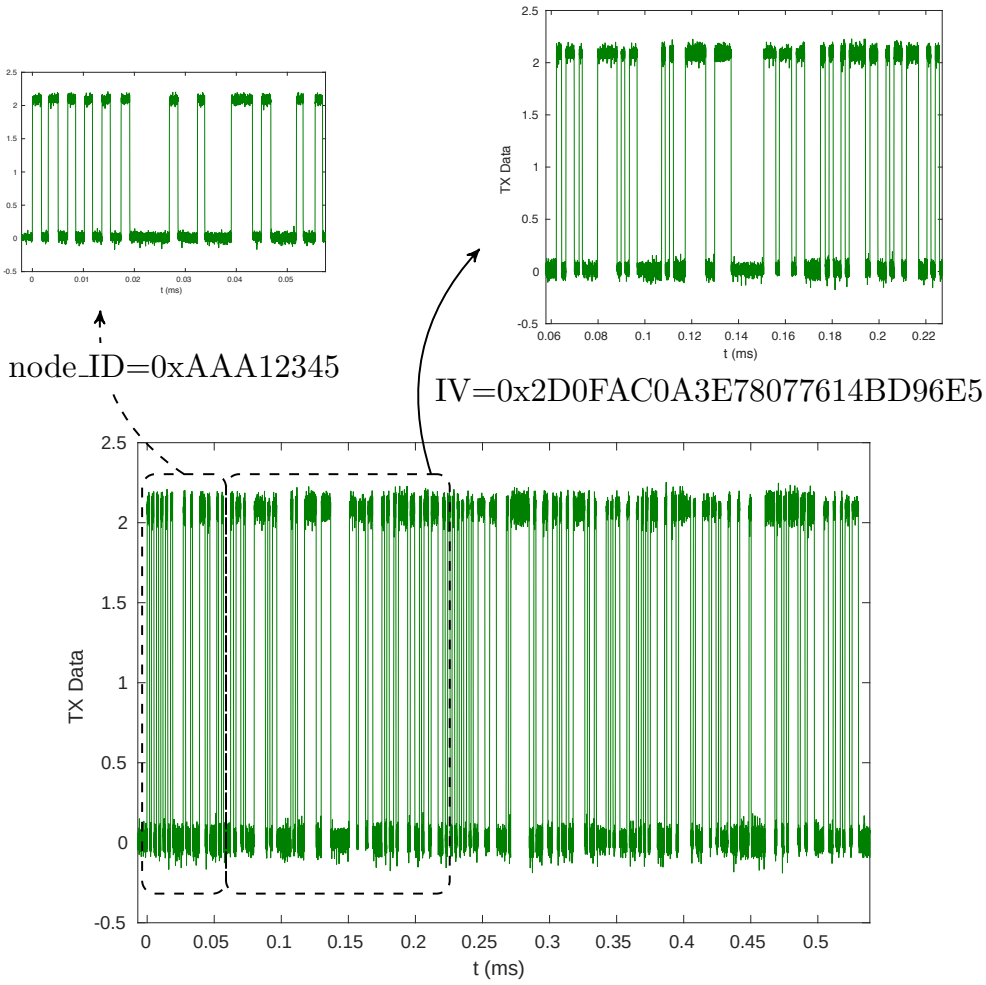


Figure 4-12: **Measured packet bits.** The figure shows a zoomed-in view of one packet in the burst transmission against time and zooms-in further to show the node ID and the IV.

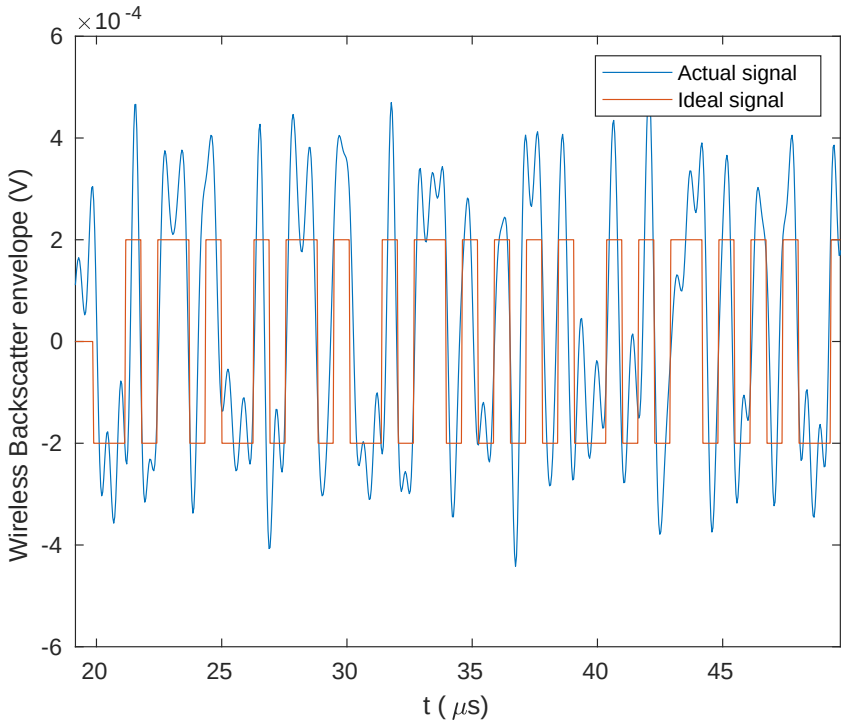


Figure 4-13: **Transmitter Uplink Measurement.** The figure plots the zoomed-in FM0-encoded wireless backscatter waveform against time (blue) along with the ideal signal (red) for the same nodeID of 0xAAA12345.

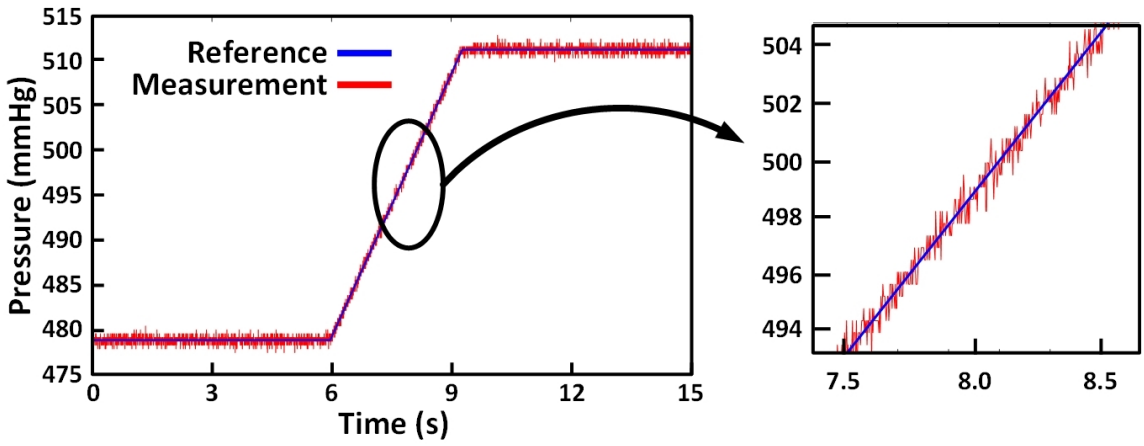


Figure 4-14: **Pressure Sensing Measurement.** The figure plots the measured digital output pressure against time (red) along with the reference signal (blue) for the same input and zooms in on where the input steps across different values.

4.4.5 Sensor Front-end characterization

The sensor front-end amplifies the input signal, cancels the offset, quantizes the data into 10-bit samples. Fig. 4-14 plots the measured transient waveforms for a continuously running setup of the sensor front-end. As shown in the figure, the 10-bit output digital code follows the input reference pressure values as it steps inside the front-end dynamic range. Analyzing the long term stability of the sensor front end, Fig. 4-15 shows the DC measurement of a fixed pressure input for a duration of four hours for two different gain configurations. The lower gain mode ($G = 100$) achieves a standard deviation of $\sigma_{G,low} = 1.4$ mmHg while the higher gain mode ($G = 1000$) attains a deviation of $\sigma_{G,high} = 0.9$ mmHg.

The front-end operates from a 0.55V supply and consumes a 1.65μW providing a 4.29nJ/conv. step. The front-end resolution is 1.37mmHg with a figure of merit ($FoM = \frac{Power}{f_s \cdot resolution} = 5.9$ mmHg·nJ/conv. step) lower than the state-of-the-art FoM meaning that our design provides a more efficient and a more accurate measurement. Table 4.1 compares the proposed sensor front-end with the state of the art pressure sensing front-ends.

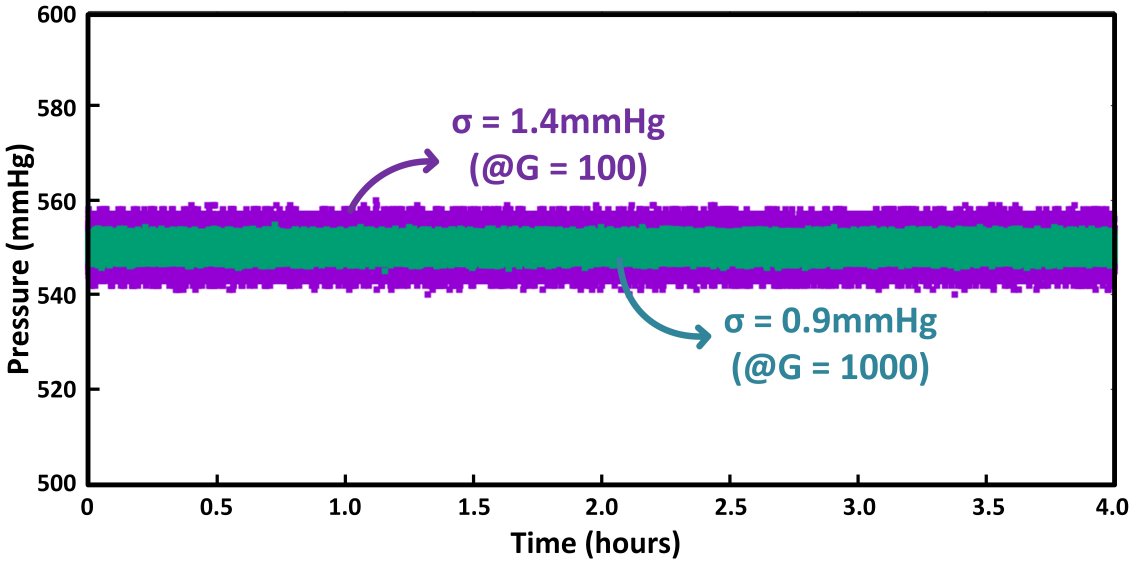


Figure 4-15: **Long term stability.** The figure plots the measured long term pressure against time for a low gain (purple) and a high gain (green) configurations showing a resolution of 1.4mmHg and 0.9mmHg respectively.

Table 4.1: Comparison of the Sensor front-end with the state of the art

Specification	**This Work**	[86]	[79]	[87]	[88]
Supply Voltage (V)	0.55	3.6-4.2, 1.2	1.9	1.2, 3.6	1.35
Power (μW)	1.65	8.52	100	2.65	35.6
Energy/Conversion (nJ/conv.)	4.29	68.1	100	10.6	8290
Resolution (mmHg)	1.37	0.3	0.78	1.1	0.67
Pressure range (mmHg)	0-2000	90-900	400-1200	100-900	0-60
FoM (mmHg·nJ/conv.)	5.9	20.43	78	11.66	5554.3

4.4.6 TRNG characterization

In order to characterize the TRNG performance, the 96-bit IV is extracted from the transmitted packets and each two IVs are concatenated to form a 192-bit sequence. A total of 5000 streams of bits is then fed to the NIST recommended tests of randomness [89] to assess its performance. Table 4.2 summarizes the pass rate of the tests recommended for short sequences of size $n > 100$ where the recommended success rate for 5000 streams of 192 bits is approximately 98.56% (4928/5000 binary sequences). The TRNG passes the NIST recommended tests for short sequences, however, we also need to demonstrate that it passes the tests with long recommended input sizes.

Table 4.2: NIST recommended randomness tests performance

NIST Pub 800-22, rev. 1a, 2010 Randomness Tests	**Pass rate**	**Percentage**
Frequency	4940/5000	98.8%
Block Frequency	4978/5000	99.56%
Cumulative Sums	4954/5000	99.08%
Cumulative Sums	4960/5000	99.2%
Runs	4947/5000	98.94%
Longest runs of ones	4945/5000	98.9%

4.5 Conclusion

This chapter presents a secure self-reconfiguring SoC of a fully-integrated wireless platform for batteryless in-body pressure sensing applications. With a reconfigurable RF front-end, the SoC can adapt to different surrounding media while its low power analog front-end with offset cancellation can continuously extract the pressure bio-data. Additionally, an on-chip AES-GCM security engine is employed to ensure data confidentiality as well as provide a means for transmitter authentication while a chaos-map based TRNG is used to generate a unique IV for each burst of backscatter transmission.

Chapter 5

Authentication, Privacy, and Control Logic of in-body Pressure-sensing Implant

While chapter 4 presented the circuit description of the main building blocks of our in-body pressure sensor, this chapter highlights the operation of the on-chip security protocol, describes the ADC sharing between the TRNG and the security engine, and then, provides the state machine for the on-chip control logic.

5.1 Biomedical data security

In-body implants are becoming more ubiquitous with the advancement of electronics technologies as well as sensor design research. With the employment of tiny sensors inside the human body, comes the challenge of security. An employed node must guarantee the confidentiality of the vital biodata being sensed and transmitted through the body or over the air. At the same time, most of these nodes will provide a means of actuation or drug release mechanism such as the case in insulin pumps. Therefore, the designed communication protocol must ensure communication authenticity such

that only an authenticated user such as the doctor or the designated patient can trigger the node to release the drug or perform its health-related task. To address such requirements, we incorporate an on-chip security engine that provides the means for transmitter authentication as well as data encryption on both the uplink and downlink.

5.2 Security Engine

This section describes the operation of the AES-GCM security engine for authentication, decryption, and encryption [90]. It also describes the design of the proposed chaos-map based analog TRNG and how it is integrated with the security engine[1].

5.2.1 AES-GCM Operation

The operation of AES-GCM is illustrated in Fig. 5-1. It provides a block-cipher mode of operation for a continuous stream of input data. It uses the TRNG to generate an initialization vector (IV) for the protocol at the beginning of each transmission event. Then, it uses a shared key (K) with the IV to encrypt the input data blocks, using the 128-bit AES encryption algorithm, to ensure data confidentiality. Additionally, it uses the node ID and the IV as additional authenticated data (AAD) along with the length of the raw data in order to generate an authentication tag ($Auth_{tag}$) which is used to guarantee the authenticity of the transmitting node. The security engine performs this counter mode of authentication by employing a Galois field (2^{128}) multiplication ($Mult_H$) to implement the the GHash function which produces the authentication tag as shown in Fig. 5-1.

[1]The security engine was designed in collaboration with Utsav Banerjee.

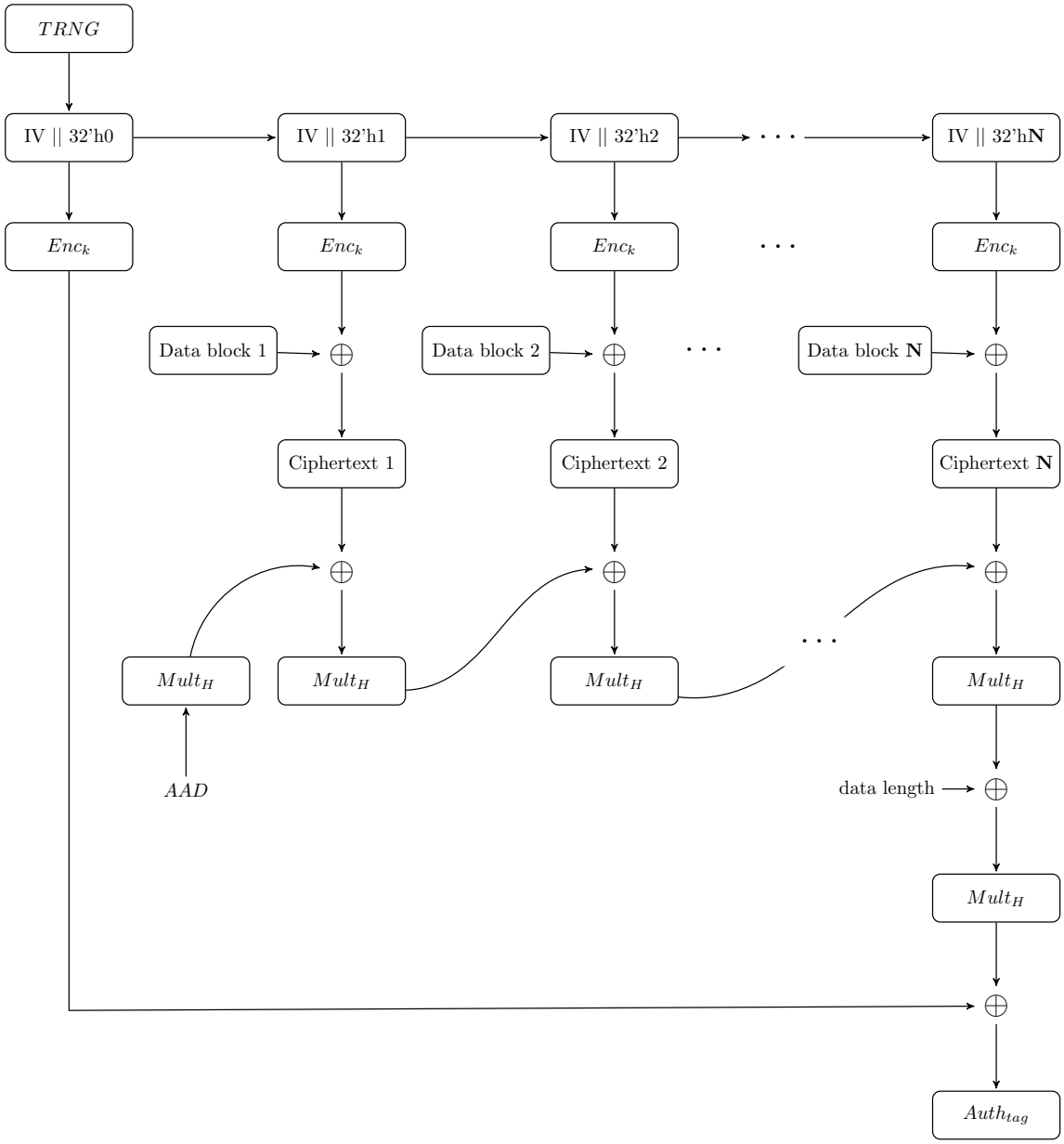


Figure 5-1: **AES-GCM protocol.** The figure shows the block diagram of the authentication and encryption operation in the AES-GCM protocol.

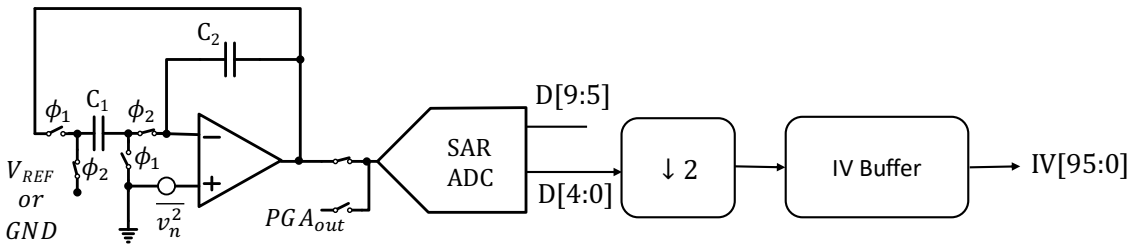


Figure 5-2: **Chaos-map based TRNG chain.** The figure shows the TRNG circuit and how it is connected to the ADC front end for the IV generation.

5.2.2 Generating the initialization vector

The AES-GCM standard states that the internal block-cipher invocations can be pre-computed if the initialization vector as well as the data length were predictable or known by an adversary node. Therefore, the generation of the IV poses a challenge to guarantee uniqueness as well as enough randomness in the string itself to ensure security and confidentiality in the protocol.

To address this, the proposed chip employs a chaos-map true random number generator (TRNG) to generate a thermal-noise-based random analog signal (as described in details in section 4.3) which is then sampled by the front-end SAR ADC which multiplexes between the pressure sensor data and the TRNG as illustrated in the single-ended version of the circuit schematic in Fig. 5-2.

5.3 Burst-mode transmission

In order to support continuous sensing and prevent the ADC from losing any samples during encryption or transmission, we propose a burst-mode transmission scheme. In such scheme, the downlink command is formed of a single encrypted packet as shown in Fig. 5-3 where the packet contains the node ID which determines which node is being addressed, the donwlink IV needed for the decryption, the encrypted donwlink command, in addition to the 128-bit authentication tag. Similarly, the uplink packet follows a similar structure with the difference that the encrypted payload has a

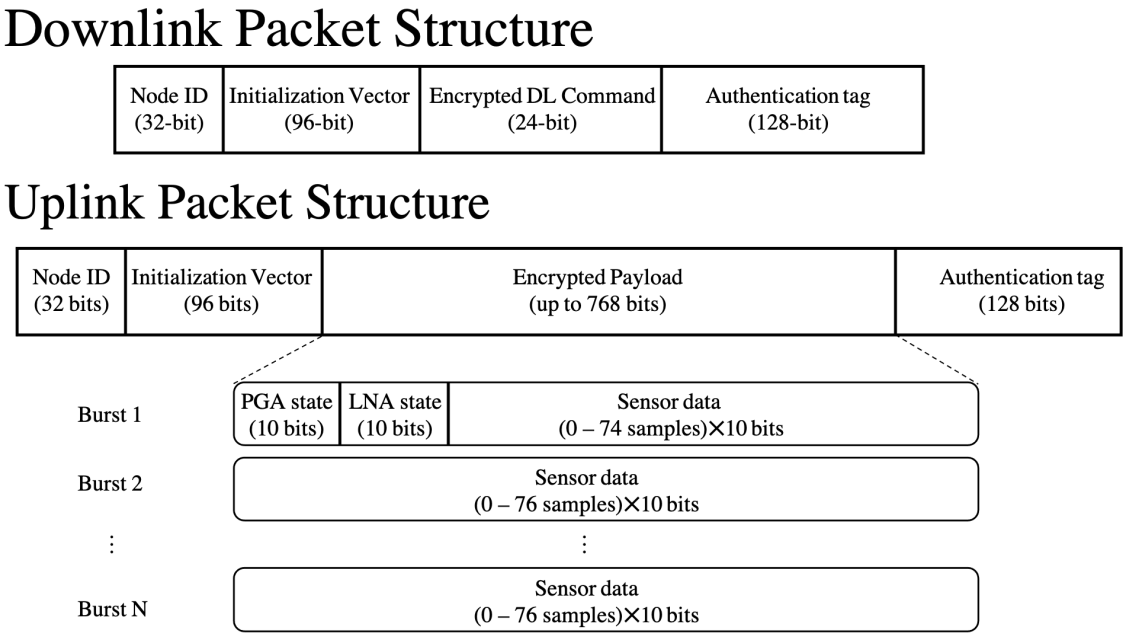


Figure 5-3: **Packet Structure.** The figure shows the downlink and the uplink packet compositions and how the uplink packet payload is divided during burst-mode transmission.

variable size which can be programmed from one 10-bit sample and up to 76 samples per packet.

For the sensor front end to operate without losing data, we employ a burst-mode of transmission where the sensor front end ADC is continuously supplying a stream of sensor data samples while the security engine starts encryption once a full 128-bit block of data is ready. To pipeline the operation, a dual-FIFO (First in first out) buffering scheme is used as shown in Fig. 5-4 where the security engine keeps enqueuing the encrypted blocks till one burst is completed and adds the authentication tag to it. The backscatter transmitter then dequeues the bits serially with the required data rate while the security engine switches to enqueue in the second FIFO preventing any sample losses.

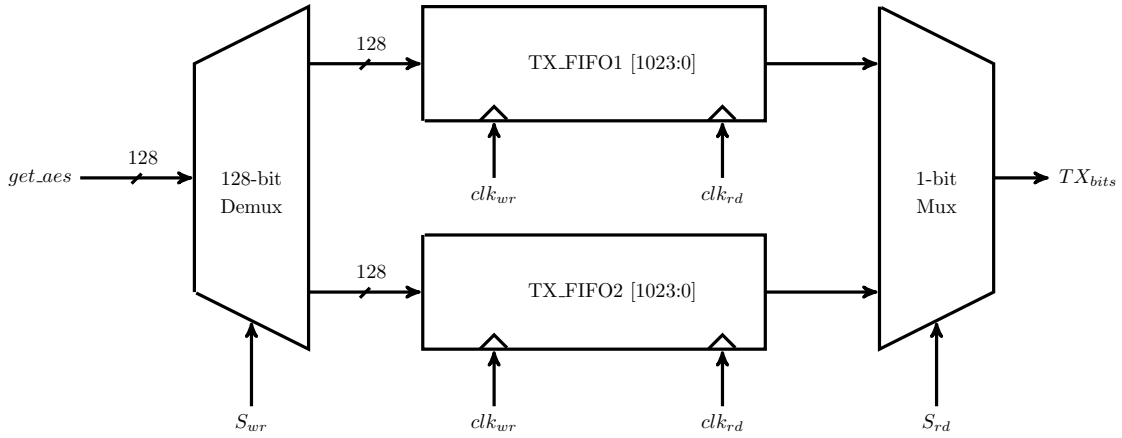
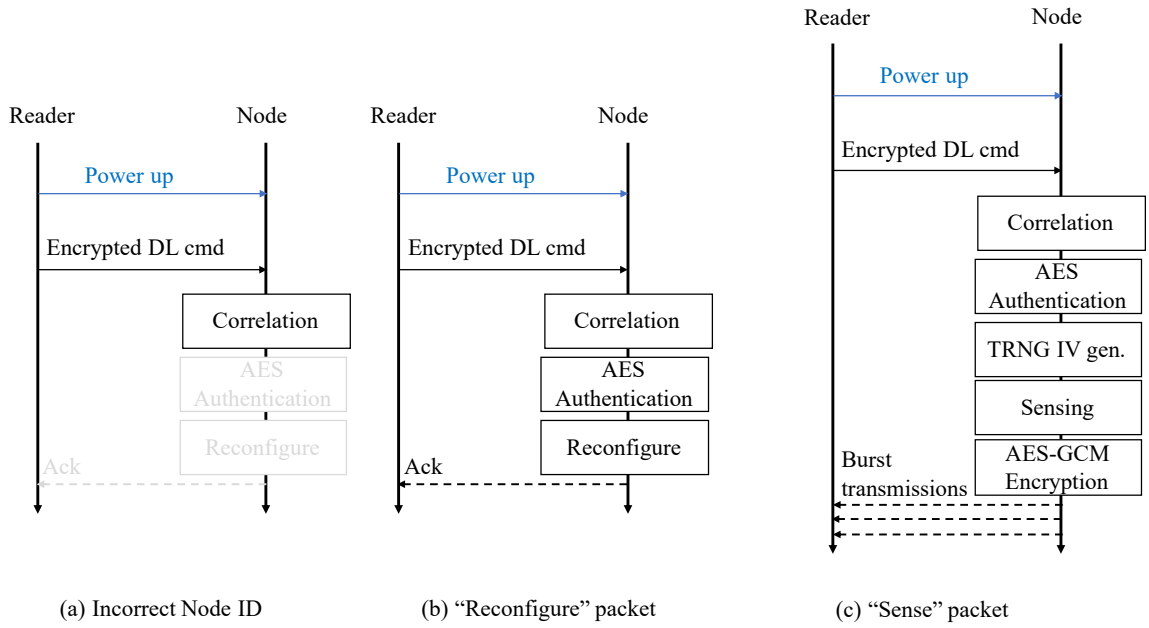


Figure 5-4: **Burst mode buffers.** A dual FIFO architecture is adopted in order to pipeline the sensor data streaming with the encryption and backscatter transmission.

5.4 Control Unit State Machine

The protocol from the downlink all the way to the uplink follows different scenarios according to the incoming bits over the RF signal. Such scenarios, illustrated in Fig. 5-5, take the logic through different branches of the state machine depending on which portion of the packet was correct or the downlink command itself. The first scenario arises when the incoming packet has an incorrect preamble, Fig. 5-5(a), then the node stops and goes back to receive and decode new bits. The second, Fig. 5-5(b), occurs when the the donwlink packet is a "Reconfigure" command sent to reprogram the RF or sensor front ends, while the third is the "Sense" command, Fig. 5-5(c) where it goes through all states from correlation, decryption and authentication, IV generation, sensing, encryption, and finally, encoding and transmission.

The state machine for the chip operation is depicted in Fig. 5-6 where the chip starts in the *Charge* state with the rectifier collecting the RF energy into DC power over the storage capacitor. Once the harvested voltage V_{DC} crosses the on threshold V_{ON}, the LDO turns on allowing for the receiver to decode the incoming bits over the RF envelope. The chip stays in the *Receive* state till it correlates with a full 20-bit



(a) Incorrect Node ID (b) "Reconfigure" packet (c) "Sense" packet

Figure 5-5: **Downlink to uplink protocol.** Different scenarios of operation for (a) an incorrect node ID packet, (b) a correct "Reconfigure" packet, and (c) a correct "Sense" packet.

preamble and then stores the 280-bit packet (as outlined in Fig. 5-3) and passes it to the AES-GCM block for decryption and authentication.

5.4.1 Downlink operation

The downlink packet transient progression through states is further described in Fig. 5-7 showing the charging, turning of receiver and then loading the 280-bit packet (RX_reg_LOAD). Following this, the AES-GCM is enabled (with an active low signal), the hardwired 128-bit key is loaded, and then the decryption starts ($EN\_decrypt\_rx$). The logic then waits for the interrupt signal that marks the end of decryption, checks the authentication flag signal get_auth, and then either go back to the *Receive* state or proceeds to perform the requested downlink command whether through the *SENSE* state, $Reconfig_{RF}$ state, or $Reconf_{sense}$ state according to the decrypted message.

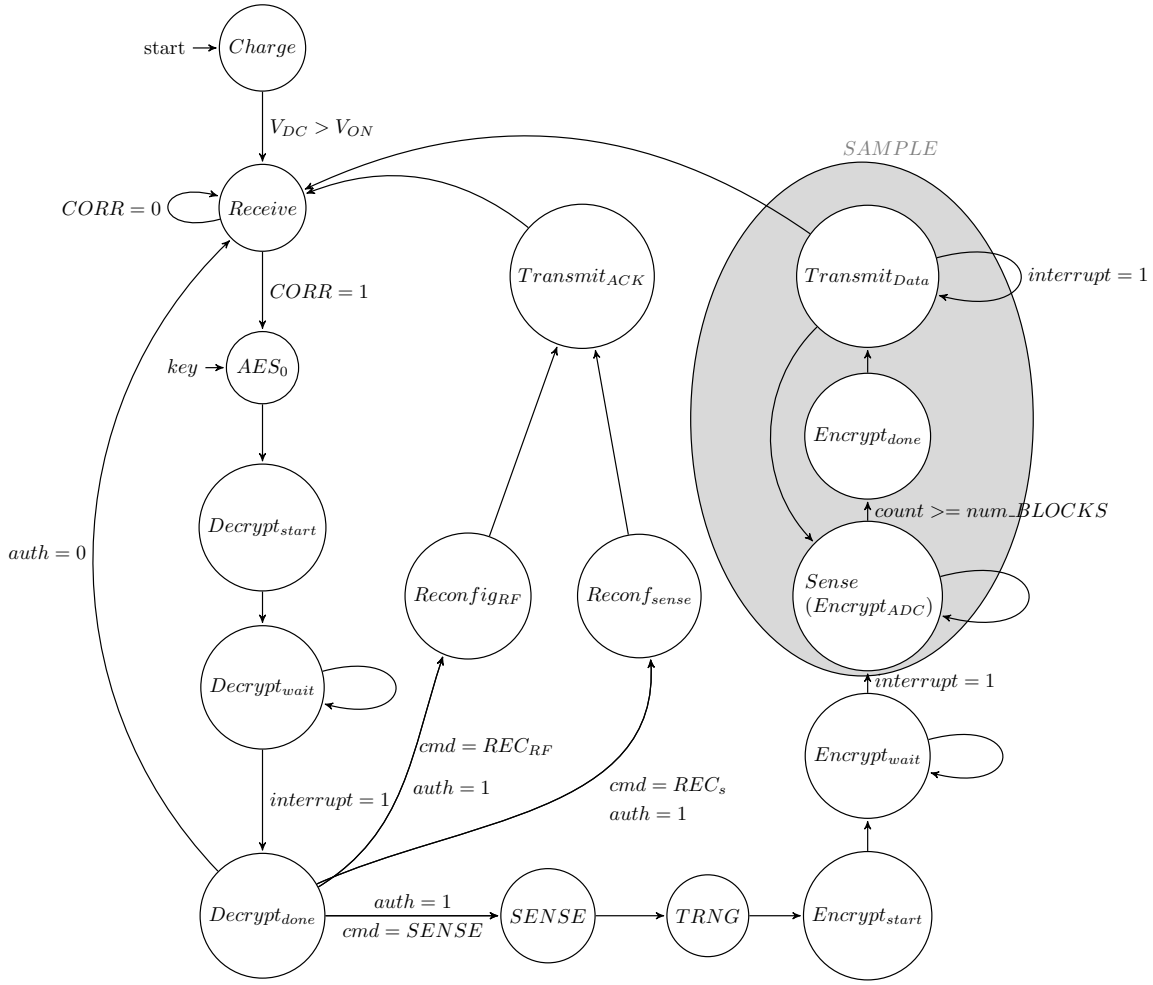


Figure 5-6: **Chip State Machine.** The chip goes through different states according to the encrypted incoming packet.

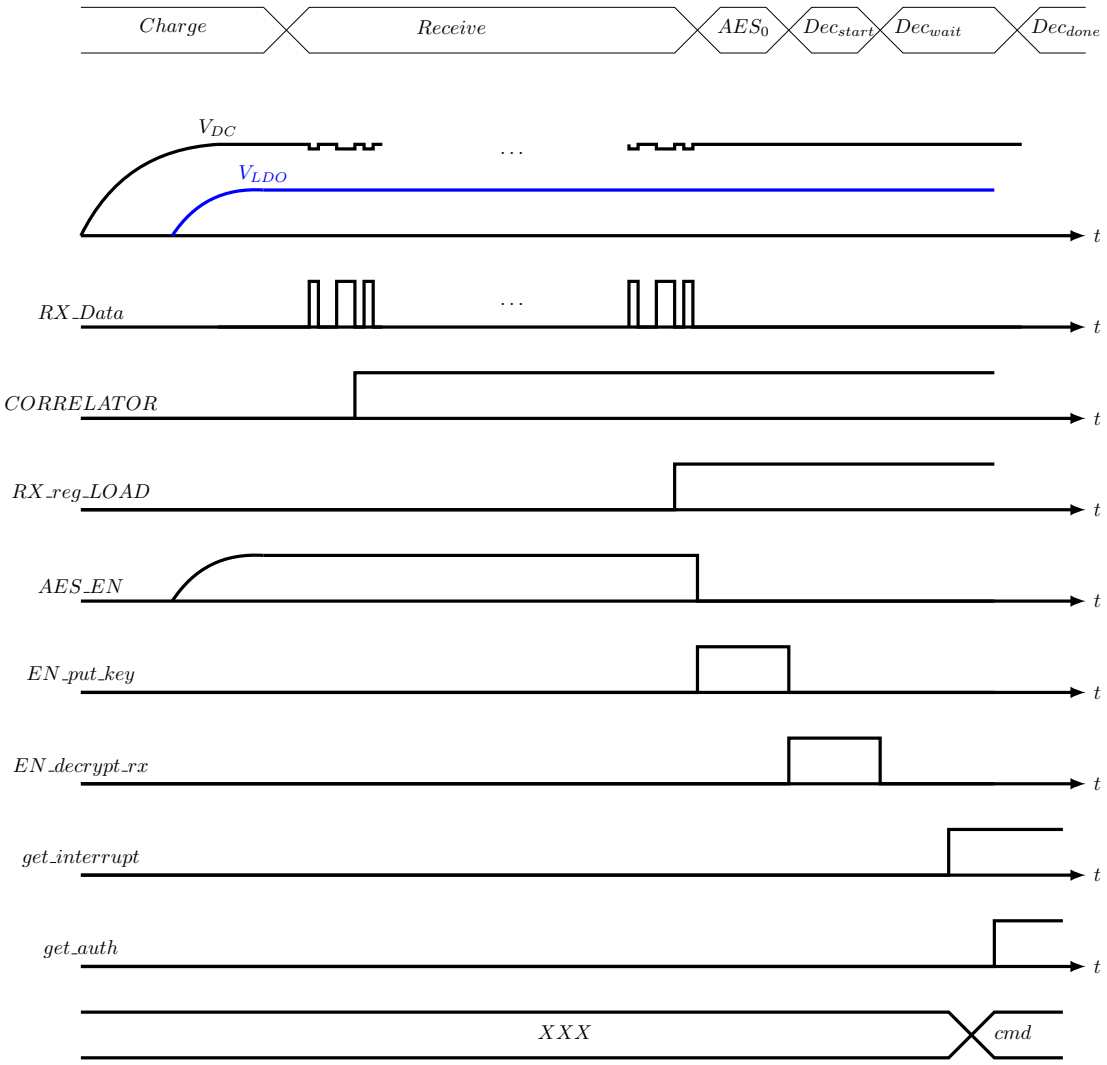


Figure 5-7: **Downlink transient operation.** The logic progresses from one state to the other generating the necessary control signals for the downlink packet decryption and authentication.

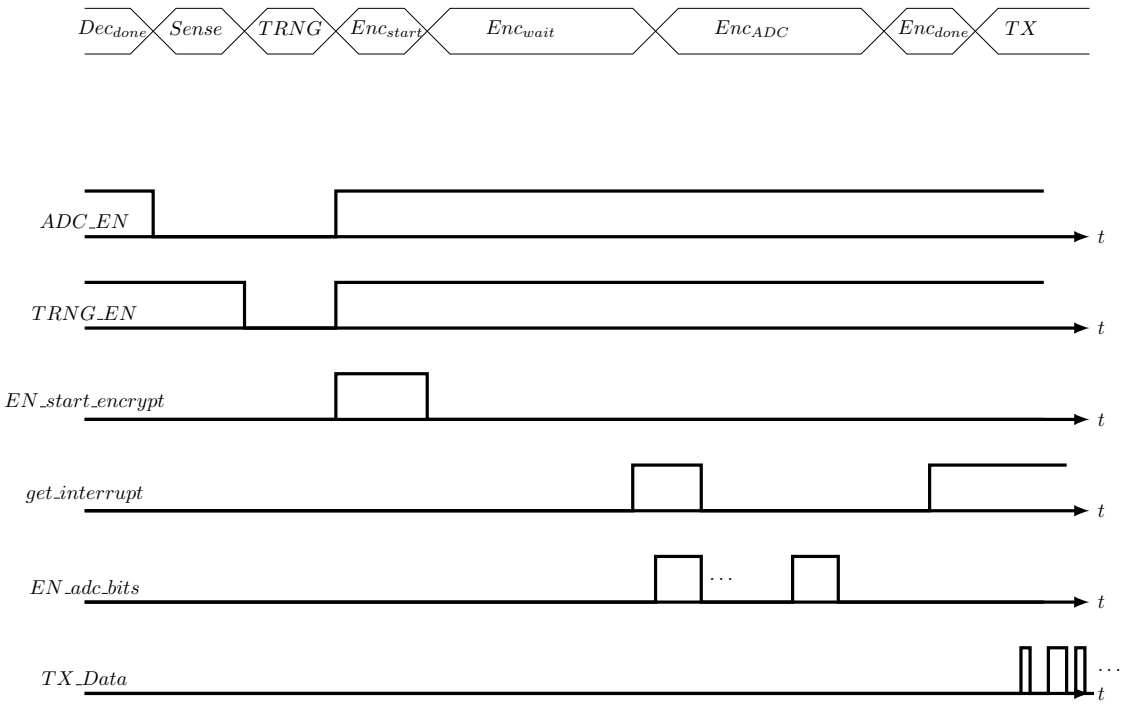


Figure 5-8: **Uplink transient operation.** The control unit enables the ADC to collect data, the TRNG for the IV, then moves to encryption and transmission.

5.4.2 Uplink operation

Once the decrypted command is determined and the logic goes into the sensing path, it follows a sequence of states and control signals outlined by the transient operation depicted in Fig. 5-8. First the ADC is enabled, and after the DC-cancellation loop finishes and the front-end settles to its steady state DC conditions, the TRNG is enabled to sample the IV bits. Following the filling of the IV buffer, the encryption operation starts ($EN\_start\_encrypt$) till it gets the configured number of data blocks and passes the encrypted message along with the authentication tag to the FM0 encoder of the backscatter transmitter chain as previously explained in details in section 5.3.

The full chip magnified die photo is illustrated in Fig. 5-9 outlining the main building blocks such as the reconfigurable RF front-end, the pressure sensing front-end,

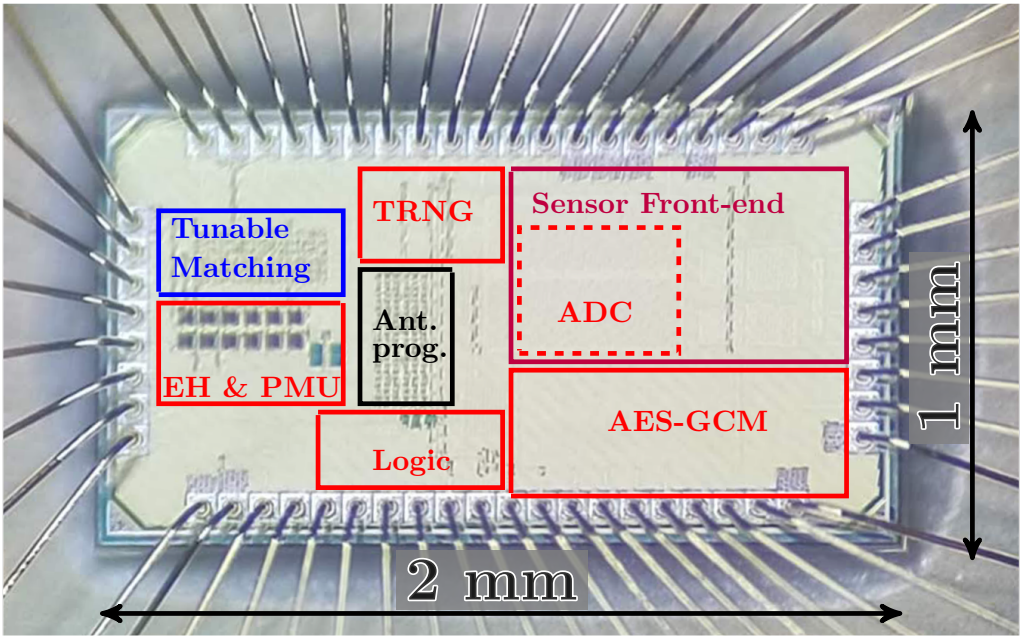


Figure 5-9: **Magnified Die Photo.** A 2×1 mm^2 CMOS chip in 65nm CMOS process showing the RF front-end, the sensor front-end, the security engine, the top level logic, and the shared ADC blocks.

the AES-GCM security engine, the logic finite state machine, as well as the shared ADC block.

5.5 Conclusion

In this chapter, we discussed the underlying reasons for data privacy and transmitter authentication. In this work, we presented the use of an AES-GCM mode with a shared secret key in order to employ transmitter authentication as well as data encryption and decryption. The chip control unit moves the chip across different states during the uplink and downlink processing while an analog chaos-map based TRNG is proposed to provide the random IV required by the security engine.

Chapter 6

A high-sensitivity BLE-compliant Wake-up receiver

So far, the previous chapters have focused on the design of in-body implants. In this chapter, we focus on the question of integrating our low power transceivers with existing standards in commercial IoT networks.

6.1 Introduction

With billions of devices expected to be connected together through the internet of things (IoT), ultra low power communication becomes the main challenge for such energy constrained devices. Ubiquitous IoT nodes usually employ a duty-cycling scheme in order to increase their life expectancy to tens of years through long periods of ultra low power sleep with short power hungry active intervals. Wake-up receivers (WuRx) act as the interface between the IoT nodes and the users where they monitor the medium for on-demand wake-up commands while the IoT node is asleep. Simple energy detection architecture appears as the best candidate for low power wake-up receivers especially in the nanowatt power consumption. However, Bluetooth Low Energy (BLE)-compliant wake-up systems utilizing energy detection such as [91]

and [92] are limited in sensitivity. The work in [91] achieves 236nW consumption while the sensitivity is limited to -56dBm. It is targeted for latency in the order of seconds where each packet constitutes only one symbol of information. On the other hand, the work in [92] achieves around 100μs latency for a sensitivity of -58dBm. It consumes 164μW with a 2-dimensional wake-up scheme. Several other designs achieve sub-μW consumption but inconveniently dictate the use of custom On-Off keying (OOK) transmitters in order to wake up the sleeping nodes [93, 94]. This work shows a BLE-compliant wake-up receiver with a -80dBm sensitivity consuming power down to 240nW and latency as low as 200μs depending on system configuration. This is achieved through a) a receiver employing passive mixer-first architecture, low power bandpass filter-based FSK demodulators and digital correlators consuming a total of 230μW for -80dBm sensitivity, b) a duty-cycling scheme and packet structure built around BLE advertising channels trading-off latency (up to 12s) and power (down to 240nW) while maintaining low false alarm rates below 1 in 1000 seconds, and c) a bit-level duty cycling of the local oscillator to further save 24% of the active power. If operated without BLE standard compliance constraints, the average power drops to 17 nW and is almost limited by the 10 nW leakage power of the design.

Section 6.2 describes the system architecture and the duty-cycling protocol while section 6.3 illustrates the measurement results and section 6.4 provides a conclusion[1].

6.2 System Architecture

Fig. 6-1 shows the system architecture with detailed circuit diagrams[2]. A free-running on-chip LC oscillator drives the mixer switches to downconvert the BLE advertising packets (at channel 37) to the IF blocks where the signal undergoes amplification

[1]The work on this chapter builds on the design outlined in [95] and moves on to perform the testing, characterization, and implement the system level duty-cycling for the BLE advertising protocol

[2]In collaboration with Arun Paidimarri.

and a 1 MHz band-pass filtering. The filter is a 4-path switched capacitor filter such that each path is driven by a single phase of four non-overlapping clocks generated by an 8-bit digitally controlled ring oscillator fine tuned according to the system IF, nominally at 4 MHz. Then an FSK demodulator decodes the input bits while a comparator with an oversampling ratio of 3 feeds three banks of correlators to search for the device wake-up pattern (WuP). If the input matches the sequence, the correlator output then exceeds its threshold and produces a WU signal to the sleeping IoT node. The 3x oversampling ratio accounts for baseband synchronization with the transmitter.

With the use of data de-whitening, the BLE advertising packet payload can hold any arbitrary user data. This work proposes a programmable datarate design which eases the circuit constraints such as the local oscillator (LO) variations as well as system level sensitivity. A programmable-size bit repetition technique can be used to programmably alter the datarate of transmission according to the system level specification where a data bit of '1' is transmitted as '111' for 3× bit repetition lowering the datarate to 333kbps instead of the BLE standard 1Mbps. Lower datarates allow for more point averaging, and hence, an effective smaller noise bandwidth. This allows the system to trade-off the transmission rate to achieve better sensitivities at lower data rates.

6.2.1 BLE compliance and dutycycling

Fig. 6-2 shows the format of the BLE undirected advertising packet indicating the possibility of embedding a wake-up sequence of up to 31 octets inside the advertising data (AdvData) of the packet. Although BLE uses a deterministic whitening pattern on the payload, a user can counteract this by pre-coding the AdvData as shown in Fig. 6-2. Thus, there is full control over 31-octets modulated with ±250 kHz Frequency Shift Keying (FSK) at 1 Mbps. Since wake-up radios are triggered on a correlation

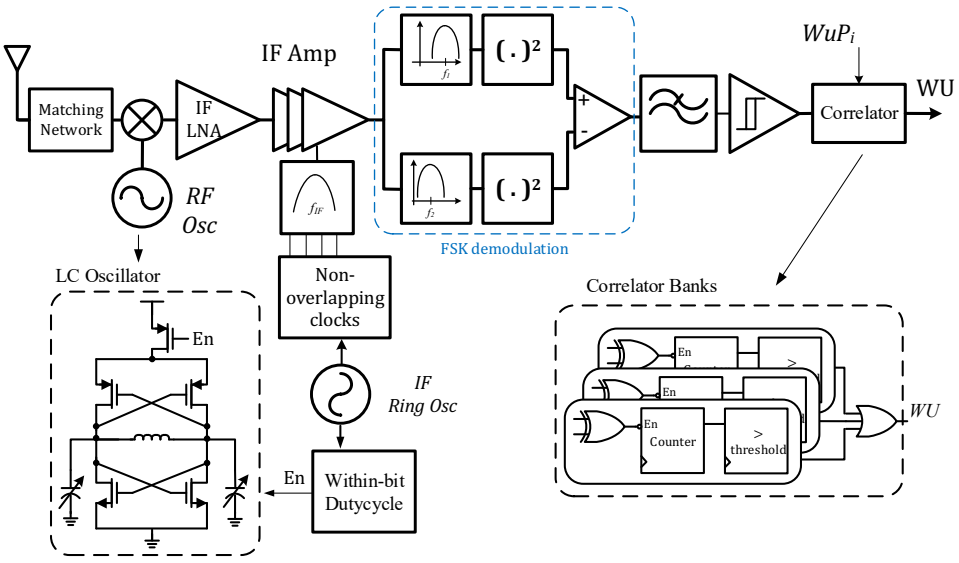


Figure 6-1: **BLE Wake-up Receiver System architecture.** The figure shows the mixer-first architecture for the wake-up receiver with the dutycycled LC oscillator and tunable IF chain.

with a full sequence of symbols, bit-repetition could be used to effectively slow-down the rate of individual symbols, thereby easing circuit design and improving sensitivity. This does trade-off false-alarm rates (FAR) due to the finite payload length. For instance, 40 kbps allows only 10 bits of WuP, and leads to unacceptable FAR, while 80 kbps works well in duty-cycled operation and 166/333 kbps work well in low-latency operation.

Different duty-cycling schemes can be employed for the FSK wake-up receiver. For a custom transmitter continuously transmitting the WuP repeatedly, then the receiver has to be on for a time (T_{ON}) equal to at least two packets to guarantee correlating to the full sequence. In contrast, a standard BLE transmitter only sends advertisements periodically, with intervals of 20ms up to 10.24s. The WuRx now needs to be on for TON of at least the advertising interval to catch the signal. Therefore, both schemes allow duty cycling to trade-off power with latency as shown in Fig. 6-2.

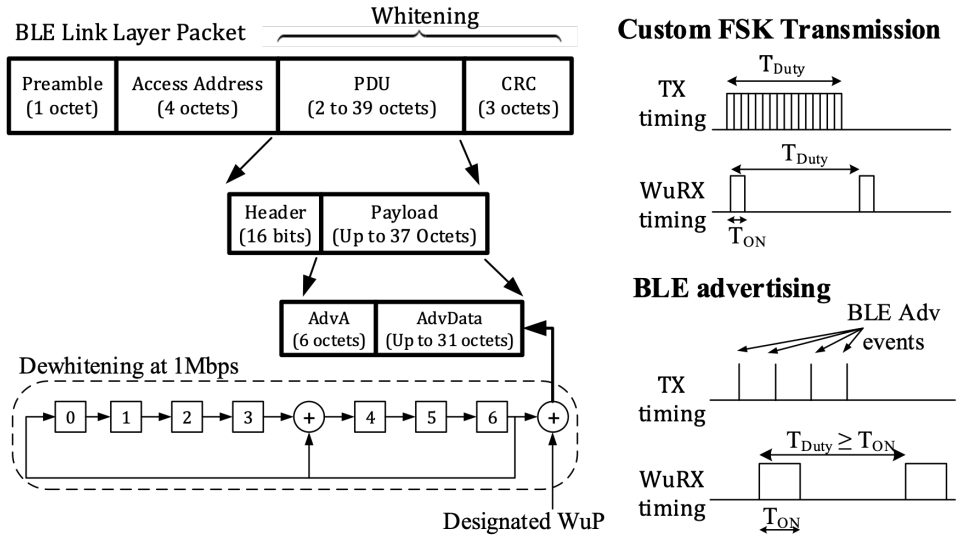


Figure 6-2: **BLE Packet structure and Duty-cycling.** The figure shows the BLE advertising packet as well as the proposed two modes of duty-cycling.

6.2.2 Within-bit dutycycling

Operating at the 2.4 GHz band, the WuRx consumes an active power of 230μW from a 0.75 V supply. The LC oscillator and its buffers consume 192μW which corresponds to about 83% of the total active power of the receiver. One merit of using a lower data rate is that each bit is transmitted for a longer time. In this system, each bit can be as long as 12μs for a data rate of 83 kbps. At such low data rates, the LC oscillator has enough time to be turned off and on during one bit transmission while still resolving the correct output at the correct sampling instances.

Within-bit duty-cycling technique is implemented where the oscillator is turned on for 66% of the cycle in order to guarantee it has enough time to settle. Such technique provides 33% savings in the oscillator's average power consumption when the receiver is active and reduces the total active power to 175.2μW. Despite having unreliable output during the oscillator off-time within each bit where the output might randomly toggle, the 3x oversampling guarantees that two samples lie within the active time of the oscillator. Hence, one of the sampled outputs correctly follows the input bits while reducing the overall average power of the receiver.

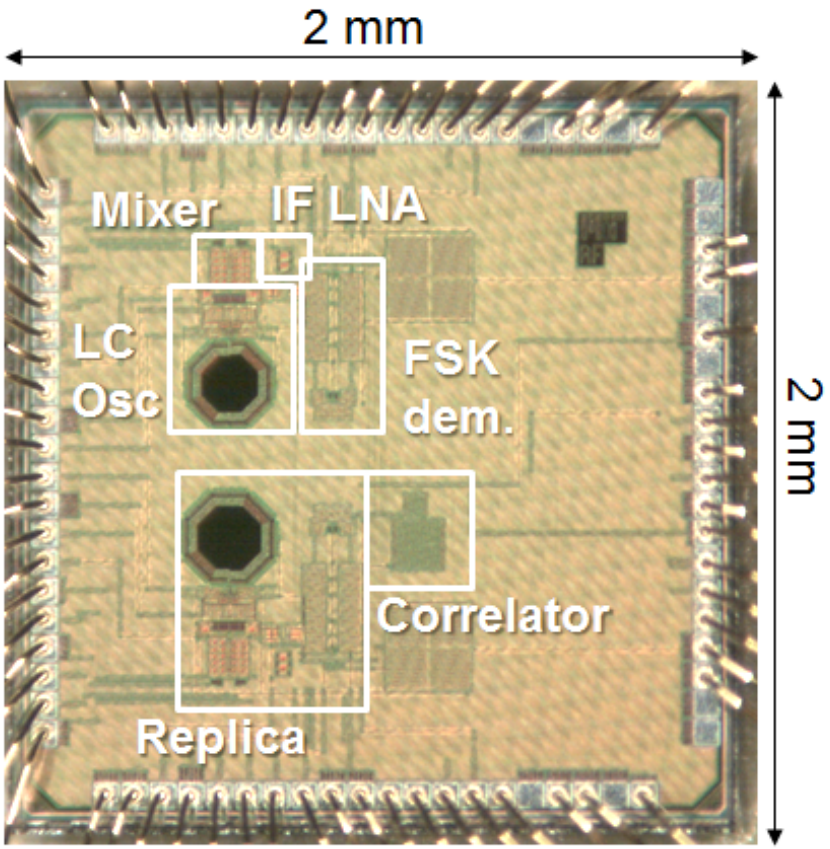


Figure 6-3: **BLE Wake-up Receiver Die photo.** A magnified image of the 2×2mm^2 chip which taped-out in TSMC 65nm process with two different LC oscillators.

6.3 Measurement Results

The chip was fabricated in a 65nm CMOS process occupying an active area of 0.48mm^2 with on-chip inductors as shown in the die photo of Fig. 6-3. This section describes in detail the measurement setup as well as the measurement results characterizing the performance of the wake-up receiver and highlighting the scalability in the presented duty-cycling scheme.

6.3.1 Measurement setup

The measurement setup is shown in Fig. 6-4 where a commercial cell phone is used to trigger the wake-up commands by embedding the node-specific wake-up sequence in

Figure 6-4: **Wake-up Receiver Test Setup.** The test chip is integrated wit an Opal Kelly FPGA board to provide the serial interface while a cellphone with a commercial BLE advertising app is used for transmission.

its advertising packet payload. Bit repetition as well as data de-whitening allows for testing the chip performance under different datarates in a BLE-compliant transmission while a custom FSK transmitter was used in the non-BLE measurement setup to explore the lower power limits of the duty-cycled receiver.

6.3.2 Receiver sensitivity

The raw receiver sensitivity is defined as the minimum input power required to achieve a bit error rate (BER) of better than 10^{-3} with a continuous random data transmission.

Trading-off Datarate for Sensitivity

With the programmable datarates and output averaging, a 3x bit repetition achieves a sensitivity of -76dBm at a datarate of 333kbps as shown in Fig. 6-5. Increasing the bit repetition up to 12x lowers the datarate to 83kbps while improving the sensitivity down to -80dBm. At lower datarates, the sensitivity improves, however, the bit repetition is limited by the advertising packet data payload and the minimum size of the wake-up sequence.

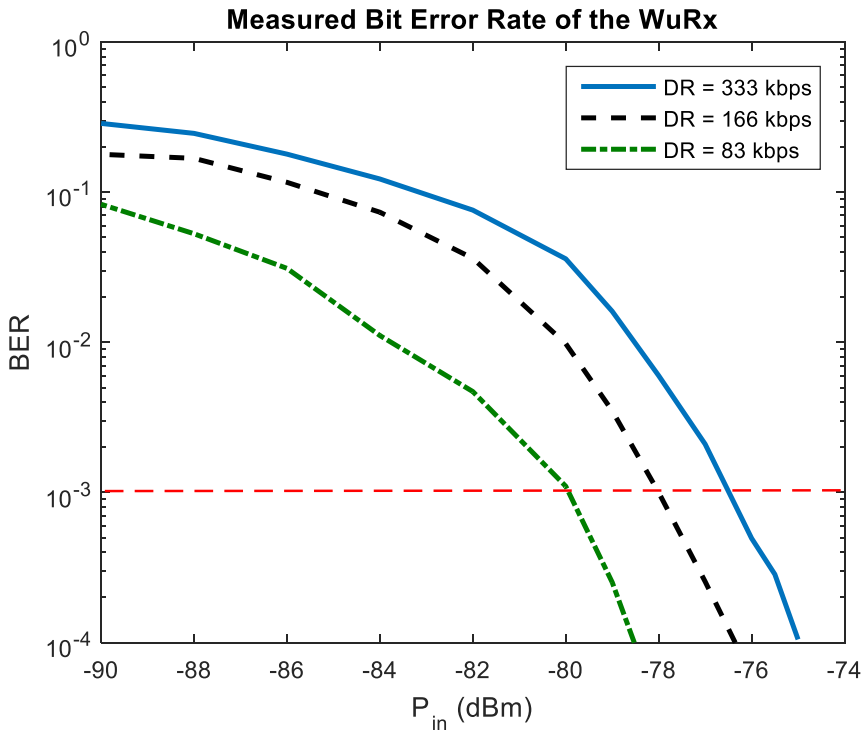


Figure 6-5: **Wake-up Receiver Raw Sensitivity** The figure plots the BER against the input power and shows how to trade-off lower rates for better sensitivity.

Trading-off False alarms for Sensitivity

Another trade-off knob in the programmable architecture is the correlator threshold used to determine the decision to trigger a wake-up event. With a full-length correlation to a 40 bit sequence at the median datarate of 166kbps, the sensitivity is -78dBm at a false alarm rate of less than once per month. Fortunately, for applications that can tolerate some level of false alarms where the correlator allows for some errors in the received wake-up sequence, then the sensitivity can be improved all the way to -84dBm as shown in Fig. 6-6. When duty-cycling is employed, the false alarm rate (FAR) is lowered by the duty-cycling ratio. The typical values for the sensitivity vs false alarm rates are given in Table 6.1 for an always-on operation (D=100%) and a duty-cycled operation (D=1%).

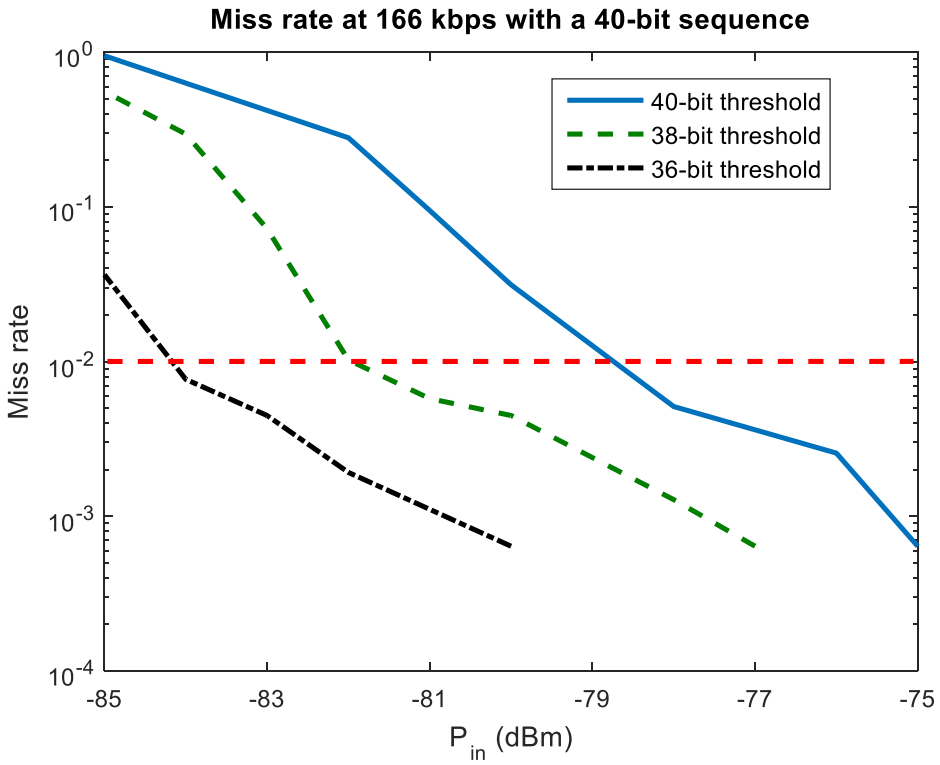


Figure 6-6: **Wake-up Receiver Sensitivity Trade-off.** The figure plots the wake-up miss rate at different correlator thresholds showing how it can be traded-off to achieve a sensitivity as low as -84dBm.

Table 6.1: Wake-up Sensitivity vs estimated FAR

Duty-cycle ratio	**Correlator threshold**		
	40-bit	38-bit	36-bit
100%	-78 dBm $<$ 1 FA/month	-82 dBm ≈1.7 FA/hr	-84 dBm ≈1 FA/4s
1%	-78 dBm $<$ 1 FA/year	-82 dBm ≈1 FA/58hr	-84 dBm ≈1 FA/7min

6.3.3 Duty-cycling modes

For each of the different duty-cycling schemes, the average power consumption as well as the latency are measured to identify the limits of each scheme.

Custom FSK Transmission

Using a custom FSK transmitter in an unbalanced link puts all the load on the transmitter where it has to repeatedly transmit the wake-up sequence till a wake-up event is triggered. Conversely, the WuRX has to be active for only the duration of two packet lengths to guarantee correlating to the full FSK wake-up sequence. Such scheme is shown in Fig. 6-7 where almost after 0.1ms, the WuRX turns on, then its oscillator settles and correctly decodes the input wireless stream to trigger a wake-up event. In this case, the average power can be as low as 17nW for an average latency of 5 seconds.

BLE always-ON transmission

For latency critical application, an always-ON BLE mode is adopted where a wake-up command can be triggered in as fast as 200μs as shown in Fig. 6-8 where the WuRX triggers the wake-up signal as soon as the correct BLE packet is received and decoded. Such scheme, trades-off the power consumption for lower latency where the average power is composed of the total active power of 230μW.

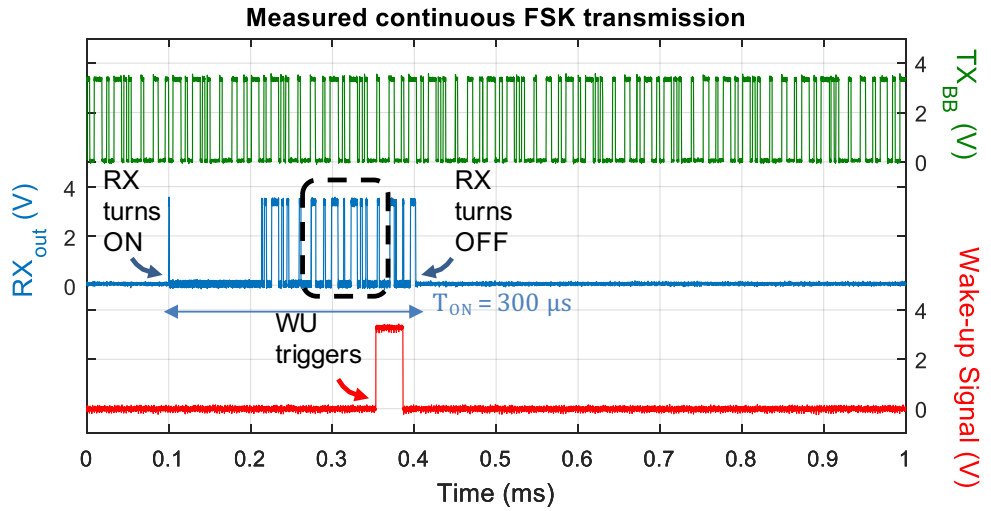


Figure 6-7: **Custom FSK Transmission.** The measured transient waveforms using a custom FSK transmitter show the WuRX operation as it turns on and triggers when a correct WuP is decoded.

BLE duty-cycled transmission

Compromising latency with power consumption, a BLE-compliant duty-cycling scheme turns the WuRX on for 25ms while shutting it off for 25s consumes only an average power of 240nW with a worst-case latency of 12.5s. The BLE-compliant operation is shown in Fig. 6-9 where a BLE packet is received midway during the on-time of the wake-up receiver and a wake-up command is triggered once a full correlation is performed over the received wake-up sequence.

6.3.4 Frequency selectivity and adjacent channel rejection

Having a channel selection filter as narrow as 1MHz provides a frequency selectivity of 100x better than conventional free-running IF architectures. Such selectivity is demonstrated in Fig. 6-10 where any packets at an offset of more than 200kHz will not trigger a wake-up event even if it is transmitting the correct wake-up sequence.

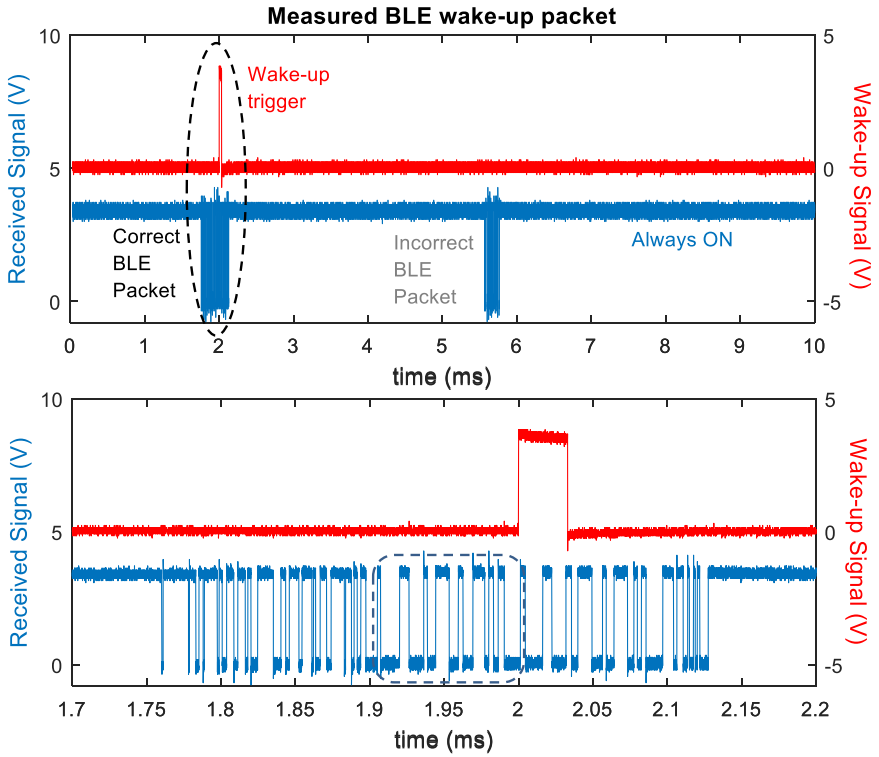


Figure 6-8: **BLE always-ON Transmission.** The measured transient waveforms of the wake-up trigger and decoded bits in the always-ON mode shows the WuRX triggering only to the correct packet which is further illustrated in the zoomed-in view.

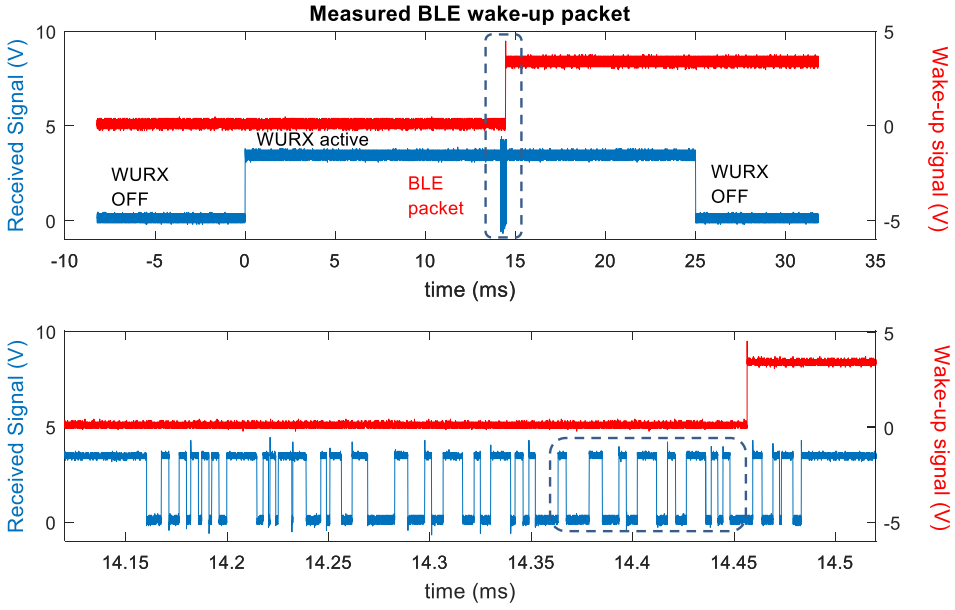


Figure 6-9: **BLE duty-cycled Transmission.** The figure plots the incoming bits as well as the wake-up trigger signal for the duty-cycled mode which provides a lower power alternative while still triggering a wake-up event for a correct BLE packet.

6.3.5 LC Oscillator stability

The frequency of an LC oscillator has been shown to be stable over a long period of time as in [94]. Similarly, by observing the frequency of an on-chip LC oscillator, it is shown that for a stable environment where no sudden temperature change is expected, the frequency remains constant within a variation as low as 50kHz during the transmission of one packet as shown in Fig. 6-11.

6.3.6 Trading-off Power with Latency

The scalable design presented in this chapter serves as a general-purpose wake-up receiver for all kinds of applications. As shown in Fig. 6-12, operating with a custom FSK transmitter, the power consumption can be as low as 17nW with a lower limit of 10nW at higher latencies. On the other hand, with the use of BLE advertising packets, a wake-up command can be triggered in as fast as the packet length of 200μs. With human-interactive applications, the latency of a few seconds can be tolerated which allow for operating at the lower end of the curve with an average power of 240nW for an average latency of 12.5s with a 20ms advertising interval.

Table 6.2 summarizes the performance and provides a comparison with other low power BLE compliant wake-up radios.

Table 6.2: Comparison with existing Wake-up receivers

Specification	**This Work**			**[93]**	**[91]**	**[92]**
Technology	65nm			180nm	65nm	90nm
Supply(V)	0.75/0.7			0.4	0.5/1	2
BLE-compliance	Yes			No	Yes	Yes
Modulation	GFSK			OOK	OOK	OOK
Carrier Frequency	2.4GHz			113.5MHz	2.4GHz	2.4GHz
Average Power	240nW	230μW	17nW	4.5nW	104/236nW	164μW
Latency	12.5s	$\approx 200\mu s$	$\approx 5s$	$\approx 90ms$	$\approx 2s$	$\approx 100\mu s$
Sensitivity	-84/-76dBm			-65dBm	-39/-56dBm	-58dBm
Datarate	83 – 333kbps			0.3kbps	8.192kbps	N/A

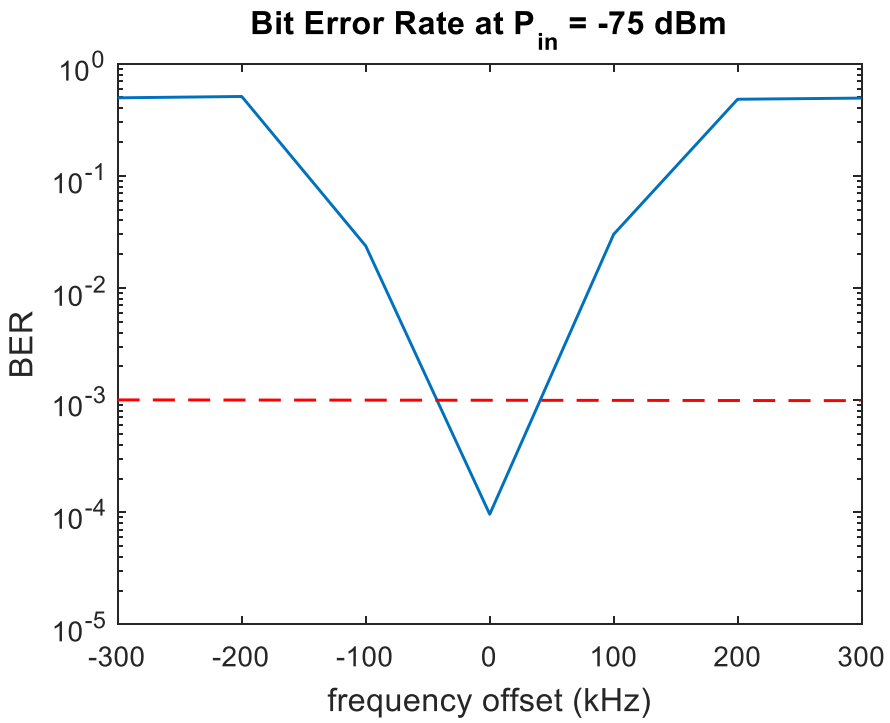


Figure 6-10: **Wake-up Receiver Frequency Selectivity.** The BER is plotted against the channel frequency offset showing showing a selectivity as low as 100kHz.

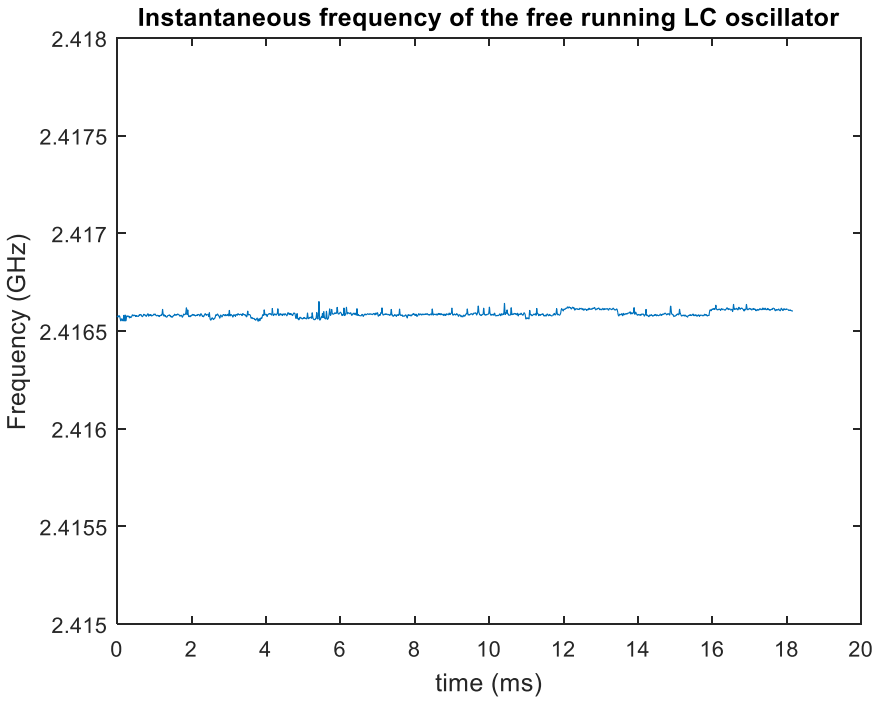


Figure 6-11: **LC Oscillator Stability.** The LC oscillator's instantaneous frequency is plotted against time to show its inherent stability compared to ring oscillators.

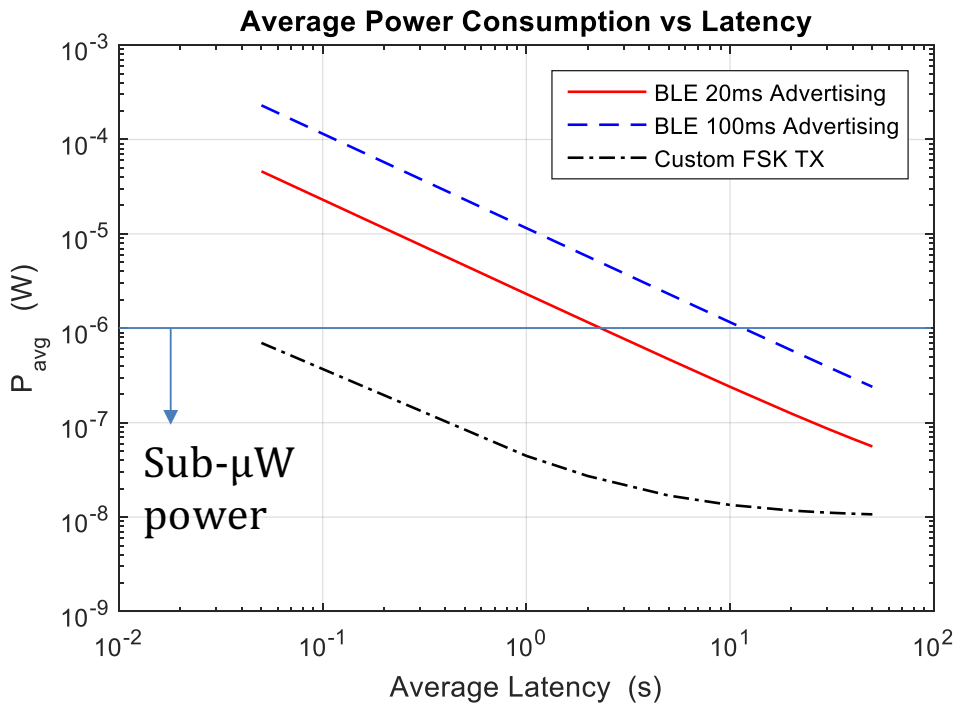


Figure 6-12: **Scalable Power and Latency.** The average power consumption is plotted against the average wake-up latency for different modes of operation illustrating how this chip can serve a wide range of applications.

6.4 Conclusion

In conclusion, this chip presents a low power duty-cycled wake-up receiver optimized to operate with conventional BLE-compliant handheld devices. With scalable power consumption as well as latency, this platform can serve nanowatt applications for battery constrained devices as well as 200μs latency critical industrial sensing applications.

Chapter 7

Transmitter Authentication using RF feature extraction

In the previous chapter, we presented a standard compliant BLE wake-up receiver for IoT networks. In this chapter, we explore the potentials of utilizing the unique RF features to identify different nodes in the IoT network.

7.1 Introduction

With the Internet of Things (IoT), all the handheld devices and ubiquitous sensors surrounding us are getting connected to the cloud. With an exponential growth, an estimate of billions of devices will be connected to the internet in just a couple of years. This dictates all of these devices to have a power hungry communication circuits to be able to send and receive data to the users or the cloud. However, most of these devices are battery operated with a low energy budget. Therefore, they usually employ a heavy duty-cycling scheme where they are asleep in a low power mode for the greatest portion of time and only wake up whenever needed for an on-demand communication.

As an interface between the users or the internet and the sleeping IoT nodes, wake-up receivers come into play where they continuously monitor the wireless signal

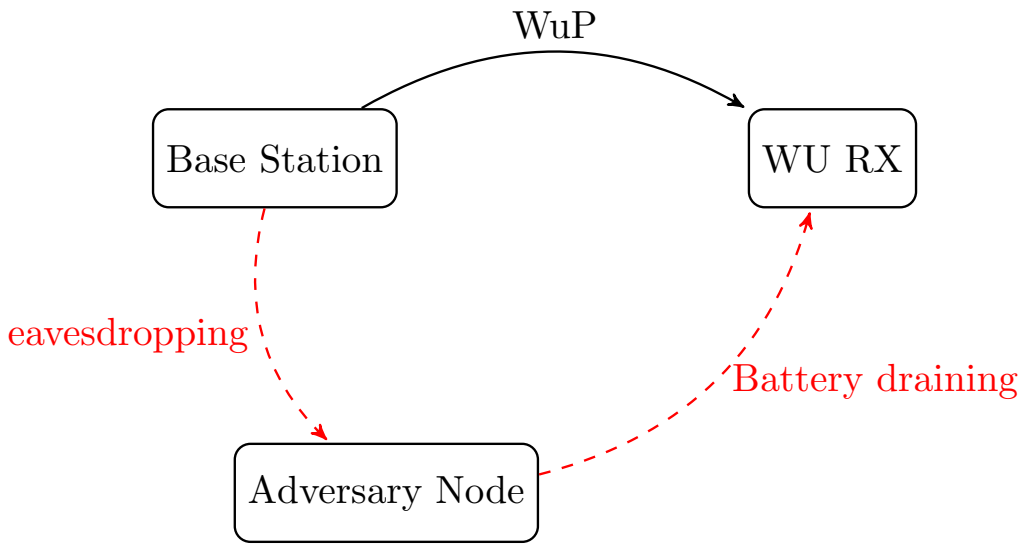


Figure 7-1: **Battery draining attacks.** An adversary node can eavesdrop the medium for the wake-up pattern and *replay* it to drain the batteries of existing nodes.

for any wake-up command from the user. Once the correct command is received, the wake-up receiver triggers the sleeping node to turn on, perform its required task, and communicate with the user.

7.2 Battery draining attacks

Conveniently enough, there has been a lot of research on designing Bluetooth-Low Energy (BLE) wake-up receivers such as the systems presented in [10] and [96]. Unfortunately, with the prevalence of Bluetooth devices, an adversary node might join the network and eavesdrop the medium for the wake-up pattern (WuP) of a specific node. As shown in Fig. 7-1, such battery drainage attacks can continuously drain the batteries of different nodes in the system till the whole network is rendered dead.

Transmitter identification as a countermeasure

A perfect candidate to prevent such attacks is to use machine learning to model each transmitter and train the wake-up receiver to correctly identify the authenticated

radio frequency (RF) transmitters from the adversary nodes. Several works in the literature tackle the transmitter identification problem through deep learning such as [97] and [98] using OFDM packets for WiFi devices while [99] identifies different IEEE 802.15.4 packets using Zigbee devices.

7.3 RF fingerprinting

This chapter builds on the previous work existing in the literature while extending it to the wake-up receiver domain to prevent battery draining attacks. In a scheme similar to [10], the transmitters wake the sleeping nodes up by embedding a predetermined wake-up sequence inside the payload of the BLE advertising packets. Here, we aim to correctly classify the label of the transmitting device given the fact that they all send the same wake-up packet to the sleeping node at a relatively varying channel in a conventional conference room environment.

The main reason why transmitter identification works is due to the fabrication uncertainty in the manufacturing process of integrated circuits. For instance, an oscillator designed to operate at a frequency of 1 GHz ends up having a statistical distribution around such nominal value across the sample space of hundreds of chips. Despite the fact that these process, temperature, and voltage variations are orders of magnitude less than their nominal value, a machine learning algorithm can learn to extract such features and filter out the common features in order to put the correct label on each packet. These unique features include:

- Oscillator frequency offset: Represents the constant frequency offset from the ideal frequency.

- Oscillator transient response: Represents the transients such as overshooting and settling time when the oscillator switches from one frequency to the other.

- I/Q imbalance: Captures the imbalance between the in-phase and the quadrature components of the input datastream.

- Power amplifier non-linearity: Manifests itself when the signal envelope varies greatly from one symbol to the other such as the case for OFDM (Orthogonal Frequency Division Multiplexing) modulation.

7.4 BLE wake-up receiver fingerprinting

Handcrafting features to feed to an ML model is an intricate task that requires understanding the origin and strength of such features. On the other hand, training a deep model to learn everything including the feature transformation is a data hungry approach which necessitates the availability of millions of samples that are not available for custom self-collected datasets for real-life problems. This section explores the performance of different hand-crafted features and proposes a new feature extraction process for an enhanced accuracy over the same dataset.

7.4.1 Measurement setup

In this setup, the self-collected dataset is comprised of 5000 BLE packets using 5 different BLE transmitters of the same manufacturer with 1000 packets per transmitter[1]. The data collection utilized the RedBear BLE nano kits [100] to encode the same exact packet in each transmitter while using a digital storage oscilloscope with a 10 GSamples/s to capture the 2.4GHz RF signals, as illustrated in a schematic of Fig. 7-2. All of these boards use the same Nordic nRF52832 BLE chip [101] in order to assess the more difficult problem of identifying the uniqueness of different chips fabricated with the same design and through the same fabrication facility.

[1]Data collection and classification were done in collaboration with Srivatsan Sridhar.

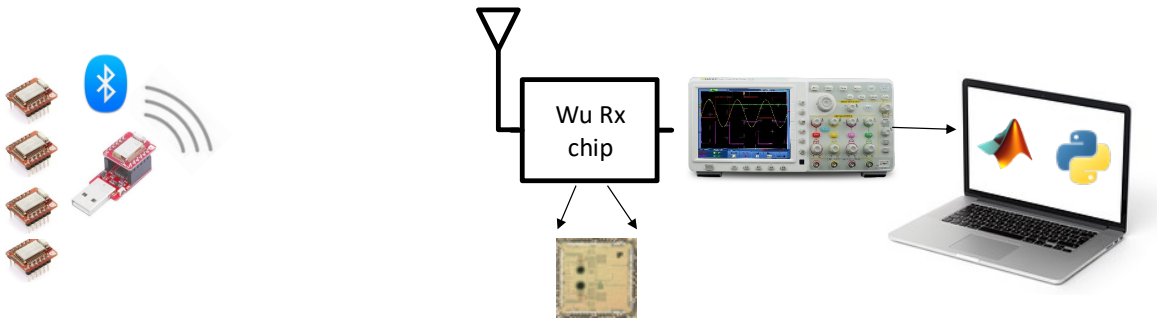


Figure 7-2: **Schematic of the test setup.** The figure shows the how the 5 BLE nano transmitters are used for the classification problem where the data is collected and processed offline after the wake-up receiver is triggered.

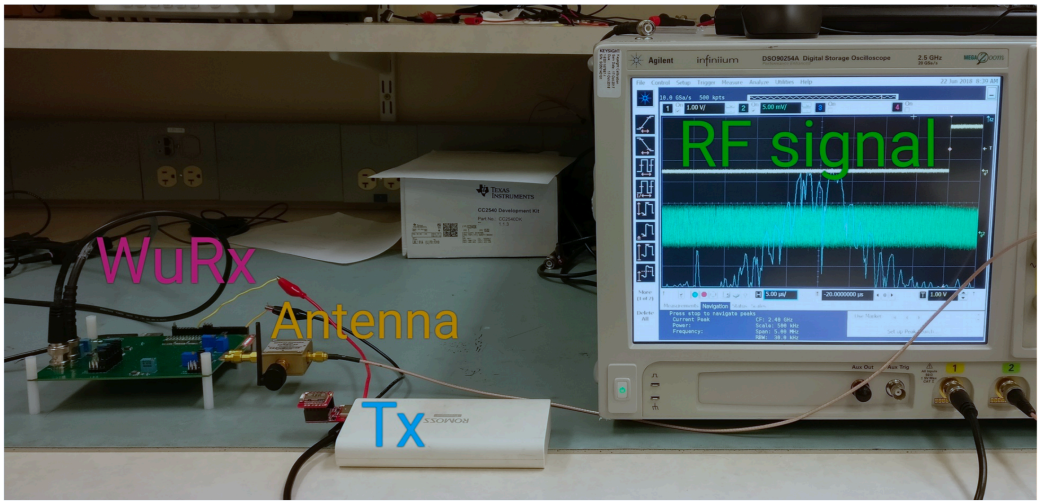
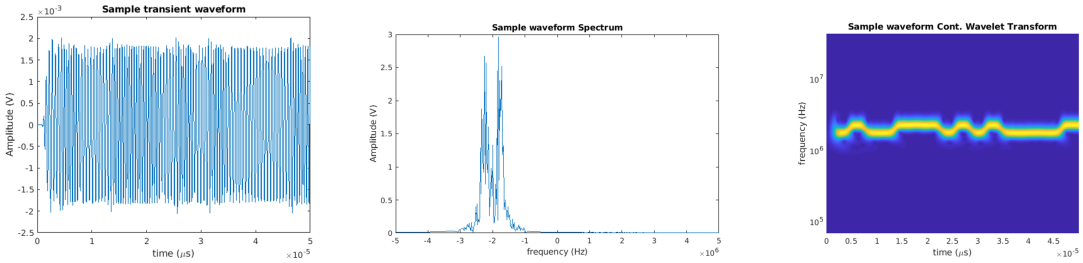


Figure 7-3: **Actual Test Setup for RF feature extraction.** A photo of the actual setup illustrates the mobility of the BLE transmitters and data acquisition using the digital storage oscilloscope.

The actual test setup is shown in Fig. 7-3 where a portable charger powers up the BLE nano transmitters to allow for a variable channel modeling while the WuRX is used to trigger the oscilloscope to store the RF signal once the wake-up pattern is received.

7.4.2 Dataset description

Each packet is downconverted from 2.4 GHz to an intermediate frequency of 2 MHz while the data is truncated to a 50μs containing the "100111010100001" bit sequence.



(a) time-domain sample (b) frequeny-domain sample (c) time-frequency sample Settings

Figure 7-4: **Dataset samples.** The figure plots samples of the used dataset in the time-domain, frequency domain, and the time-frequency map using the wavelet transform.

Sample waveforms are shown in Fig. 7-4 where it is clear that the BLE packet utilizes frequency shift keying (FSK) to transmit a '1' with a higher frequency offset while a '0' is transmitted at a lower frequency offset from the carrier frequency.

7.5 RF signal model

In the signal processing domain, there are several ways to represent an RF signal. We start by analyzing the three different representation depicted in Fig. 7-4.

- **Time-domain representation:**

  In this model, the RF signal is modeled as:

$$x_{RF}(t) = x_{BB}(t) \cdot e^{j(2\pi f_c t + \varphi_{RF})} \tag{7.1}$$

  where a baseband signal $x_{BB}(t)$ modulates a carrier signal at a center frequency $f_c = 2.4$GHz while the phase mismatch and phase noise are modeled by the random phase component φ_{RF}.

  To lower the system's sampling rate, the 2.4 GHz signal is downconverted to an intermediate frequency of 2 MHz, then a 1 MHz bandpass filter selects the BLE channel under test to filter out any out of band interferers or noise. Then, the

time-domain features are given by:

$$\phi_t(\mathbf{x}) = filter_{Bandpass}(x_{RF} \cdot e^{-j2\pi(f_c+2MHz)t}) \tag{7.2}$$

- **Frequency-domain representation:**

  This model is better in capturing the center frequency offsets where the down-converted signal at 2 MHz is transformed to the frequency domain using the discrete time Fourier transform. The frequency-domain features are given by:

$$\phi_f(\mathbf{x}) = \sum_{n=0}^{N-1} \phi_t(x_n) \cdot e^{-j\frac{2\pi kn}{N}} \tag{7.3}$$

  where N is the number of samples and $\phi_t(x)$ is the filtered signal at the intermediate frequency.

- **Time-frequency representation:**

  The last representation captures both the time domain as well as the frequency domain characteristics of the signal but is more computationally expensive and increases the input dimensionality. This model utilizes the continuous wavelet transform (CWT) to get the input signal frequency map as follows:

$$\phi_{CWT} = \int_{-\infty}^{\infty} \phi_t(x;t) \cdot h^*(\frac{t-b}{a})\ dt \tag{7.4}$$

  where a and b denote the time scales and shifts respectively. This transformation projects the input signal on different scaled and shifted versions of a mother wavelet given by a complex sinusoidal with a gaussian envelope:

$$h(t) = e^{j2\pi ft} \cdot e^{-\frac{t^2}{2}} \tag{7.5}$$

7.6 Measurements and evaluation

Using the aforementioned dataset, the three models are evaluated in a simple classification task where each packet can take a label $y \in \{1, 2, 3, 4, 5\}$ and the accuracy is used as the performance metric. The dataset is divided into three sets: 80% for training, 10% for validation, and 10% for testing.

Model description and Evaluation results

Different neural network models were trained with sizes changing from one feature vector to the other in order get the highest accuracy for each representation.

- **Time-domain model and evaluation:**

  Initially, the time-domain model gave a low accuracy around 20% similar to a random guess for a 1 out of 5 classification. But then, by aligning all the waveforms together to assist the model in the classification process and cancel out the fixed phase offset, the accuracy reaches a plateau at around 48% as shown in Fig. 7-5. In this experiment, the model was composed of two hidden layers with 1000 and 64 units respectively while the input feature vector has a length of 5000 and the output gives the probability over 5 different transmitters.

- **Frequency-domain model and evaluation:**

  The frequency domain model did much better getting an accuracy as high as 90%. However, this was due to the apparent frequency offset between the transmitters. Unfortunately, such offset is temperature dependent and can be spoofed and added/subtracted by an adversary node. Hence, learning from this model, we manually extracted the frequency offset from all packets in order to learn other inimitable features.

- **CWT model and evaluation:**

  After removing the frequency offset, the CWT model still classified the trans-

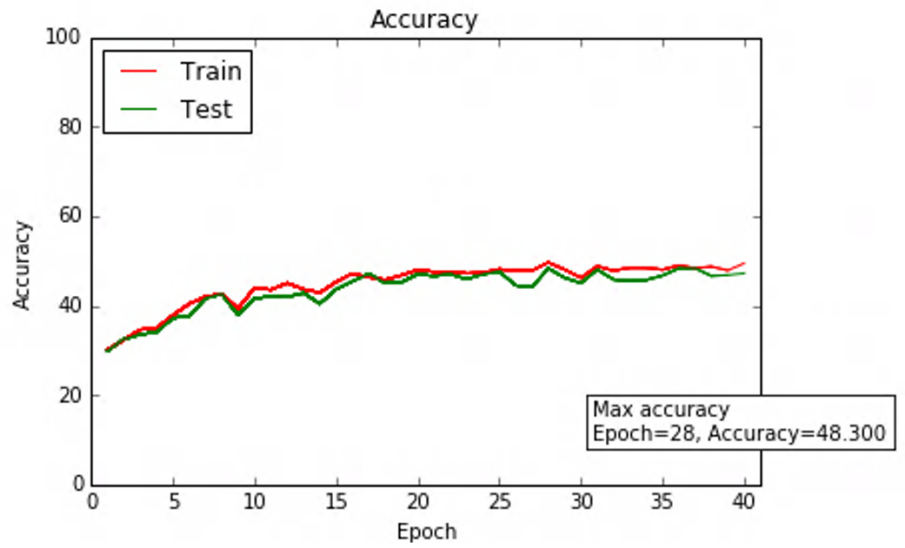


Figure 7-5: **Time-domain model identification accuracy.** The figure plots the training and test accuracy for the raw transient waveforms of the input signals.

mitters with a maximum accuracy of around 90%. Such accuracy was improved to 93% through the use of data augmentation where the training packets are augmented through negative and positive time shifts while still maintaining their unique features. This increase in the dataset helped in the generalization over the test dataset and provided an extra 3% in accuracy as shown in Fig. 7-6. The model here consisted of one hidden layer of 64 units while the input is now a 2D array of size (500 time shifts x 30 frequency scales).

7.7 Proposed feature extraction

Since the BLE packets employ an FSK signal which incorporates all of its information in the frequency components of the signal, it was intuitive to drop the amplitude information and provide a higher order model for the transient frequency response.

This section proposes the feature extraction method illustrated in Fig. 7-7 where

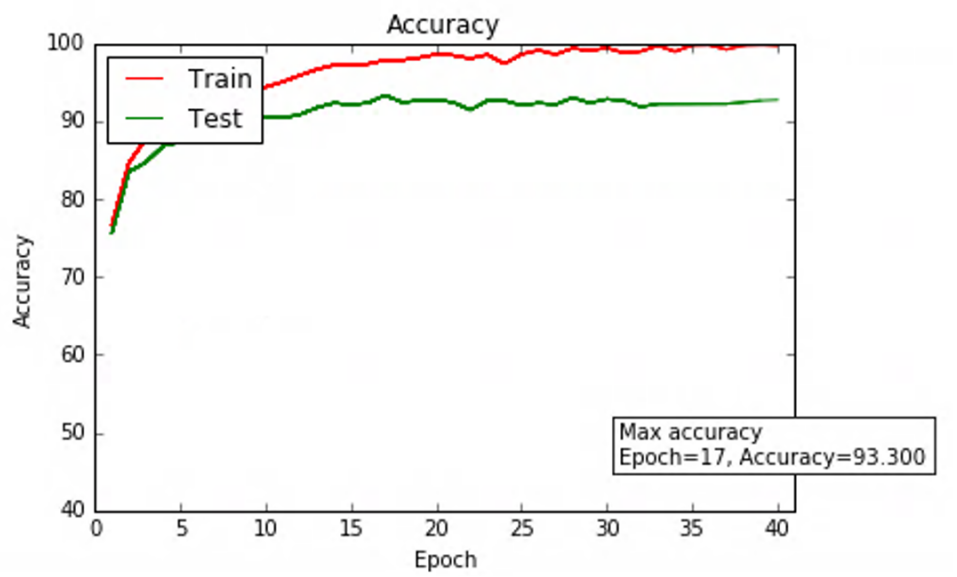


Figure 7-6: **CWT-model identification accuracy.** The figure plots the training and test accuracy for the time-frequency model showing a peak classification accuracy of 93.3%.

the transient frequency is extracted from the downconverted input signal as:

$$f(x;t) = \frac{d}{dt}(phase(\phi_t(x;t))) \tag{7.6}$$

then, the transients of the signal including its settling time, overshoot as well phase noise are captured through another wavelet transform over the transient frequency to give the following new features:

$$\phi_{proposed}(f;a,b) = \int_{-\infty}^{\infty} f(x;t) \cdot h^*(\frac{t-b}{a})\ dt \tag{7.7}$$

With a fully connected model incorporating one hidden layer with 64 units, the accuracy improves up to 95% over the conventional time-frequency map classification. In addition, the dropping of the amplitude information means that the initial time-domain signal can be quantized to only 1 bit resolution while only the extracted phase and the wavelet transform require higher resolutions.

The accuracy is plotted in Fig. 7-8 showing a peak of 95% while the confusion

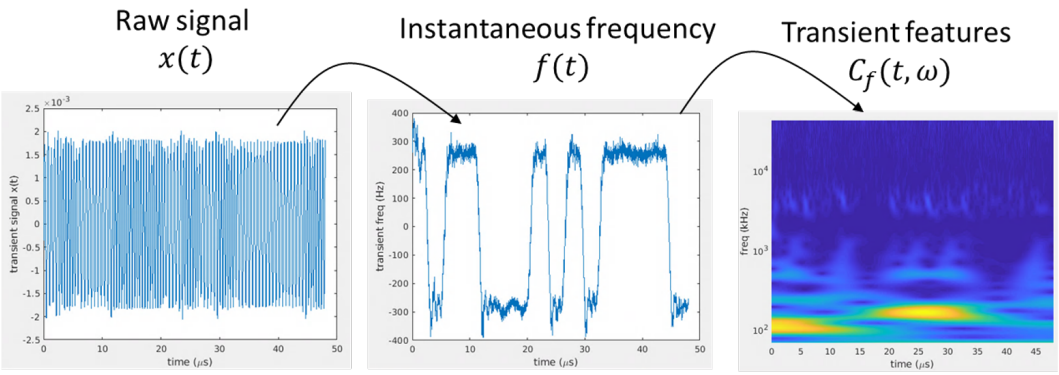


Figure 7-7: **Proposed feature extraction method.** The proposed feature extraction model extract the instantaneous frequency of the downconverted signal, and then calculates its time-frequency map using CWT.

matrix is shown in Fig. 7-9 over the five different transmitters.

7.8 Conclusion

In conclusion, using machine learning for transmitter identification proves to be beneficial for wake-up radios and IoT networks. Even with the same manufacturer

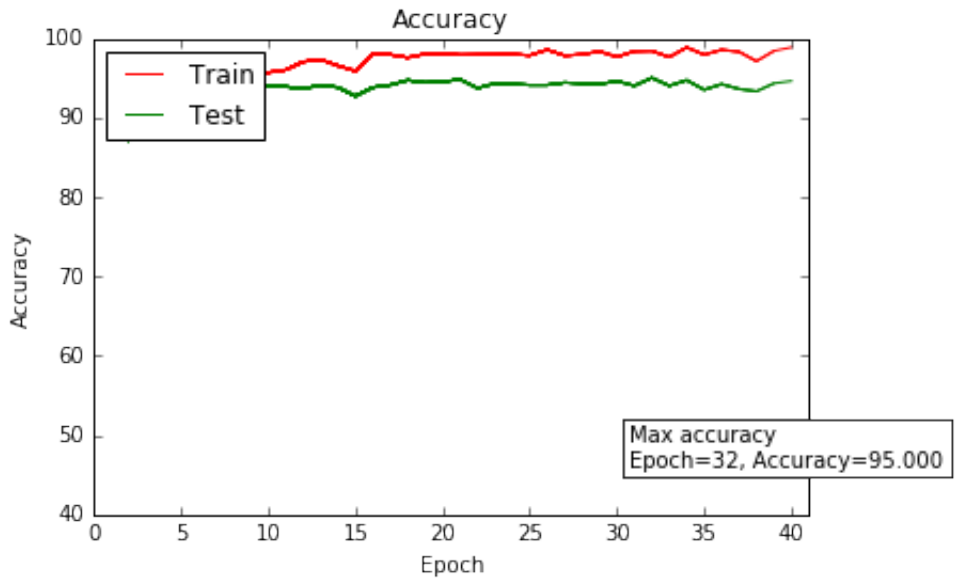


Figure 7-8: **Proposed model identification accuracy.** The figure plots the training and test accuracy of the model with the proposed feature extraction showing a peak classification accuracy of 95%.

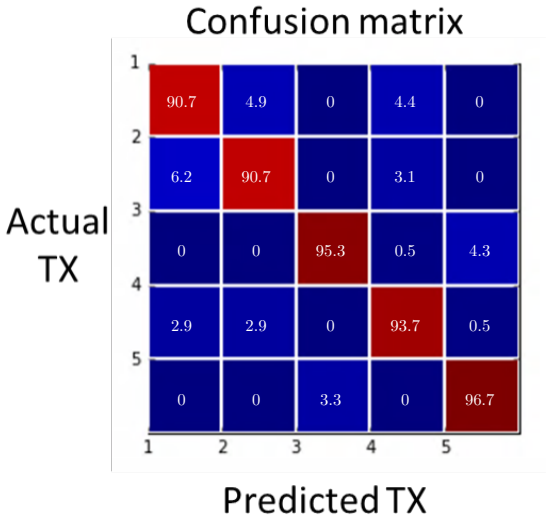


Figure 7-9: **Confusion Matrix.** The figure shows the confusion matrix for the five transmitters where the identification accuracy is more than 90% for each node..

and packet payloads, the transmitters can be identified using their instantaneous frequency transients with an accuracy as high as 95% under varying channel conditions. Frequency offset cancellation and data augmentation improved the accuracy by helping the model to learn more distinctive features and generalize to different environments and channels.

Chapter 8

Conclusion and Future work

This thesis focuses on the design of low power adaptive circuits for wireless IoT nodes and in-body implants. It attempts to break the system-level trade-offs to achieve adaptive architectures with scalable performance, standard compliance, as well as secure communication at microwatts of power consumption. In its core, the main thesis contributions lie in the design, implementation, and testing of three integrated low power reconfigurable wireless systems.

8.1 Thesis summary

In this section, we summarize the work outlined in this thesis and draw conclusions to provide a path for future work to build on the presented contributions.

Chapter 2 presented a background for the energy harvesting chain as well as the backscatter link for in-body implants while chapter 3 demonstrated μmedIC, a reconfigurable wireless platform for batteryless cross-tissue connectivity and communication. μmedIC utilizes a coupled antenna structure with a capacitor bank loading to provide a tunable antenna which can adapt to the variations arising from different surrounding tissues. Since an optimum wireless energy harvesting system employs a rectenna optimization problem where the rectifier and the antenna are co-designed for the

best sensitivity, our proposed system incorporates a programmable input impedance matching network to co-reconfigure both the rectifier and the antenna under different conditions and frequencies. The node reconfigurability extends to automatic data rate adaptation to scale down the power consumption by an order of magnitude adapting to lower input RF power scenarios. Such adaptation provides a compromise between throughput and availability depending on the application being served.

Our approach for this system was to design a general purpose platform for in-body implants wireless RF front ends. Different patients have different body compositions, and hence, over-optimizing the design for specific surrounding tissues only works for a particular patient rather than generalize to all patients. Providing reconfigurability in both the circuit-side as well as the antenna-side breaks such over-optimization problem and opens the way for a wide range of mobile implants.

Chapter 4 built on μmedIC system and presented the design of an in-body pressure-sensing node for secure wireless and batteryless sensing. This system integrates the reconfigurable RF-front-end with a custom high gain sensor front-end with a reconfigurable offset cancellation loop to extract the pressure sensor data and sample it using a 10-bit SAR ADC. The offset cancellation loop as well as RF-front-end can be reconfigured through the downlink packets providing faster settling time. A chaos-map TRNG is implemented to provide a different IV for the AES-GCM encryption operation for each transmission event. Chapter 5 explained the security aspect of the pressure-sensing node and how the control logic follows different branches for reconfiguration, authentication, decryption, sensing, or burst-mode transmission.

The key takeaway from this design is that secure batteryless operation is possible through system-level innovations as well as lower level circuit techniques. Low energy highly parallel security engine architectures provide both data confidentiality as well as authenticity through trading off active area with active power consumption. Low supply voltages ($< 0.55V$) with adequate gain and quantization can build energy

efficient sensor front ends for custom sensing applications. Finally, block reuse such as re-purposing the sampling ADC for the TRNG allows for further area and power reduction through pipelining the sampling operation with the IV generation operation.

Chapter 6 presented the circuit design of a BLE-compliant wake-up receiver as well as a duty-cycling protocol for sub-μW average power consumption while achieving better than the standard specified sensitivity. It employs a mixer-first architecture with a free-running LC oscillator while an n-path filter is used to filter the BLE advertising channel with a programmable clock to track the oscillator variations. Heavy duty cycling is employed to lower the average power in a schemed wrapped around the BLE advertising protocol allowing the average power to trade-off with latency and scale down to 240nW.

This work demonstrates that a mixer-first architecture has the potential to provide a good noise figure while consuming lower power as all amplification and filtering is moved to a lower intermediate frequency (IF). Despite the fact that a free-running oscillator suffers from frequency drift over time, our approach of a reconfigurable IF receiver chain can track such drift allowing for a small noise bandwidth ($\leq$ 1MHz) and hence, a sensitivity as good as -80dBm. Such reconfigurability is possible through the employment of n-path filters for both IF channel selection as well as FSK demodulation with a programmble ring oscillator to provide the tunable frequency.

Chapter 7 explored the radio frequency fingerprints inherent to different transmitters in IoT networks and how to use them to identify authenticated transmitters. Low power RF fingerprint extraction by wake-up receivers can be used to mitigate the threats of replay attacks with fixed wake-up commands. We proposed to use the continuous wavelet transform on the instantaneous frequency of the incoming BLE packets to extract the unique features of each transmitter's phase locked loop (PLL) as it switches between frequencies for the transmission of the FSK modulated symbols.

8.2 Lessons learned

One lesson learned from having a wide range of programmability in the antenna coupling (e.g. more than 100MHz) it that it makes the testing and deployment of such systems easier and suitable for different types of patients and applications. While the input impedance matching has to follow the same programmable range, the capacitor banks range and the switches sizing has to be carefully chosen to achieve an optimum point without degrading the quality factor at the expense of the tuning range or favoring the tunability at the expense of energy harvesting sensitivity. While reprogrammability helps the design flexibility, an important takeaway is that over the air programming can be used to close the loop between the transmitter and the implant creating a secure sensing and communication platform as well as a means to reprogram different system variables through the downlink.

Additionally, a key takeaway from the work on the BLE wake-up receiver chip is that existing standards and protocols can be incorporated in the system-level design and duty-cycling schemes to maintain compliance while drawing the path for less than 1μW of average power consumption and scaling down average power consumption against latency according to the application being served.

While the work on fingerprinting was exploratory, we ask the question whether unique RF features could be extracted from the received RF packets. We observe that different transmitters can be identified at an accuracy more than 90% even with devices from the same manufacturer and transmitting the same exact packet. Further investigation is necessary to understand how these features arise, how to amplify them in the transmitter design, or how to extract them in an energy efficient manner instead of incorporating a full on-chip neural network for authentication and identification.

8.3 Future directions

Biomedical batteryless and wireless implantable nodes form an ever-growing field with daily advancements in both the biomedical sensors, sensing and communication protocols, as well as the integrated interface circuits. The deployment of such nodes inside the human body or even as wearables still poses many open questions on integration, operation, and performance. We briefly state here some of the potential directions continuing on the work presented in this thesis.

Custom devices for energy harvesting

While the use of monolithic CMOS designs allows for ease of fabrication and system integration, breaking the sensitivity limits of 1μW (or -30dBm) requires innovation on all levels: device, circuit, and antenna level. Diode connected transistors have long been used as rectifying devices with circuit techniques to lower or cancel out their threshold voltage. On a parallel path, the advancements in device fabrication has paved the way for newer devices that achieve better subthreshold swing [102] breaking the $60mV/dec$ down towards a $10mV/dec$. These devices provide a higher current flow for smaller input voltage differences allowing for a faster turn on and a better sensitivity. Additionally, the fabrication techniques for 2D materials provides a direction to research on the optimization of flexible energy harvesting rectennas and as it alters the codesign procedure between the rectifier and the antenna. For instance, the work in [103] fabricates a MoS_2 rectifying device directly on the flexible substrate with the antenna to harvest energy from Wi-Fi networks. As our presented systems also demonstrated flexible wireless batteryless systems, we can bridge both works by integrating such new devices with reconfigurable Si chips to break-off the energy harvesting sensitivity limit.

Machine learning for antenna design

Designing microwave circuits, such as microstrip antennas, on a circuit board is a tedious iterative process. It requires the use of high frequency electromagnetic (EM) simulators for a numerical solution of the microwave structure using finite-element methods such as Ansys HFSS. Additionally, the turn around time to fabricate and test the board slows down the iterative process making it the bottleneck in the design procedure.

Several works in the literature have proposed the use of machine learning or neural networks to automate and speed up the design process. The work in [104] proposes a graph neural network which learns to simulate EM structures. Then, it is further extended to solve the inverse problem of finding the microwave circuit given certain EM specifications. A similar approach could be utilized for in-body antennas where a model would learn to simulate the EM antenna structure inside different tissues and even solve to design for an optimum design including the rectifier's parameters as inputs to the model.

Light weight security engines

While our pressure sensing node provides an authentication and encryption engine as outlined in chapters 4 and 5, the security of IoT devices and implants remains an open area of research. Dual factor authentication techniques incorporating the user's stimulation of a touch sensor was presented in [105]. On the other hand, the work in [106] incorporates a compact elliptic curve cryptography processor into a THz tag to enable a light-weight encryption and authentication functionality.

Integrated transmitter-identification neural networks

The work in chapter 7 illustrates how the unique features of each chip can be used to identify transmitters in IoT networks. Taking this a step further, a physically

unclonable function (PUF) could be incorporated to amplify the intrinsic variations and improve the classification accuracy as in the work presented in [107]. It captures the out-of-band-leakage power during the power amplifier's spectral regrowth and use it as a unique feature to identify each transmitter. Several analog or RF-based features could still be further exploited in the identification process while a light-weight neural network can be implemented on-chip to provide on-the-edge inference allowing the wake-up receiver to make an on-the-fly decision to trigger a wake-up event or not.

More generally, while this thesis presents a co-designed methodology for reconfigurable wireless systems, it also paves the way for new applications and circuit innovations from deep with the human body all the way to the over-the-air wireless protocols.

Appendix A

List of Acronyms

ADC: Analog to Digital Converter

AES-GCM: Advanced Encryption Standard - Galois Counter Mode

ASIC: Application Specific Integrated Circuit

BB: Baseband

BER: Bit Error Rate

BLE: Bluetooth Low Energy

BPF: Bandpass filter

BW: Bandwidth

CMFB: Common-mode feedback

CMOS: Complementary Metal Oxide Semiconductor

CWT: Continuous Wavelet Transform

DCO: Digitally controlled oscillator

DR: Datarate

DSB-ASK: Double-sideband Amplitude Shift Keying

FAR: False Alarm Rate

FSK: Frequency Shift Keying

IC: Integrated Circuit

IF: Intermediate Frequency

IoT: Internet of Things

IV: Initialization Vector

ISM: The industrial, scientific, and medical band

LDO: Low DropOut regulator

LNA: Low Noise Amplifier

LO: Local Oscillator

LSB: Least Significant Bit

MAC: Medium Access Control

NF: Noise Figure

OOK: On-Off Keying

PCB: Printed circuit board

PIE: Pulse Interval Encoding

PLL: Phase Locked Loop

PMU: Power Management Unit

RF: Radio Frequency

RX: Receiver

SAR: Successive Approximation Register

SoC: System on Chip

SNR: Signal to Noise Ratio

TX: Transmitter

TRNG: True Random Number Generator

UHF: Ultra-High Frequency

VGA/PGA: Variable/Programmable Gain Amplifier

VCO: Voltage-controlled oscillator

WuP: Wake-up pattern

WuRX: Wake-up receiver

Appendix B

List of Measurement Equipment

Table B.1: Key equipment used for the measurements in this thesis

RF Equipment	
RF Signal Generator	Agilent 8267C and Keysight N5183 MXG
Spectrum Analyzer	Agilent N9020A
Network Analyzer	Aglient E8362B and Keysight N5080B
Power Supplies	
Sourcemeter	Keithley 2400 Sourcemeter
Sourcemeter	Keithley 2602A Sourcemeter
Oscilloscopes	
Mixed Signal	Tektronix MSO3054
Digital Storage Oscilloscope	Agilent Infiniium DSO90254A
Software Defined Radio	
RFID Transmitter	USRP N210 with SBX daughterboard
RFID receiver	USRP N210 with LFRX daughterboard
Clock Synchronization	OctoClock CDA-2990
FPGA controller	
FPGA Platform	Opal Kelly XEM3001

Bibliography

[1] IDC, "IoT Growth Demands Rethink of Long-Term Storage Strategies." https://www.idc.com/getdoc.jsp?containerId=prAP46737220. Accessed:2021-05.

[2] "Apple watch." https://www.apple.com/watch/.

[3] "Fitbit tracker." https://www.fitbit.com/global/us/products/trackers.

[4] "National heart, lung, and blood institute." https://www.nhlbi.nih.gov/health-topics/pacemakers.

[5] Medtronic, "Micra pacemakers: Transcatheter pacing systems for bradycardia (slow heart rate)." https://www.medtronic.com/us-en/patients/treatments-therapies/pacemakers/our/micra.html.

[6] 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," *Nature biotechnology*, vol. 30, no. 12, p. 1240, 2012.

[7] Medtronic, "Pillcam colon 2 system." https://www.medtronic.com/covidien/en-us/products/capsule-endoscopy/pillcam-colon-2-system.html.

[8] X. Chen, X. Zhang, L. Zhang, X. Li, N. Qi, H. Jiang, and Z. Wang, "A wireless capsule endoscope system with low-power controlling and processing ASIC," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 3, no. 1, pp. 11–22, 2009.

[9] M. R. Abdelhamid, R. Chen, J. Cho, A. P. Chandrakasan, and F. Adib, "Self-Reconfigurable Micro-Implants for Cross-Tissue Wireless and Batteryless Connectivity," (New York, NY, USA), Association for Computing Machinery, 2020.

[10] M. R. Abdelhamid, A. Paidimarri, and A. P. Chandrakasan, "A −80dBm BLE-compliant, FSK wake-up receiver with system and within-bit dutycycling for scalable power and latency," in *2018 IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–4, 2018.

[11] A. Rosen, M. A. Stuchly, and A. Vander Vorst, "Applications of RF/microwaves in medicine," *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, no. 3, pp. 963–974, 2002.

[12] J. Kim and Y. Rahmat-Samii, "Implanted antennas inside a human body: Simulations, designs, and characterizations," *IEEE Transactions on microwave theory and techniques*, vol. 52, no. 8, pp. 1934–1943, 2004.

[13] R. Bashirullah, "Wireless implants," *IEEE microwave magazine*, vol. 11, no. 7, pp. S14–S23, 2010.

[14] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *Proceedings of the ACM SIGCOMM 2011 conference*, pp. 2–13, 2011.

[15] M. R. Yuce and T. Dissanayake, "Easy-to-swallow wireless telemetry," *IEEE Microwave magazine*, vol. 13, no. 6, pp. 90–101, 2012.

[16] A. K. RamRakhyani, S. Mirabbasi, and M. Chiao, "Design and optimization of resonance-based efficient wireless power delivery systems for biomedical implants," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 5, no. 1, pp. 48–63, 2010.

[17] R.-F. Xue, K.-W. Cheng, and M. Je, "High-efficiency wireless power transfer for biomedical implants by optimal resonant load transformation," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, no. 4, pp. 867–874, 2012.

[18] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, and J. Smith, "Inter-technology backscatter: Towards internet connectivity for implanted devices," in *Proceedings of the 2016 ACM SIGCOMM Conference*, pp. 356–369, ACM, 2016.

[19] D. Vasisht, G. Zhang, O. Abari, H.-M. Lu, J. Flanz, and D. Katabi, "In-body backscatter communication and localization," in *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, pp. 132–146, ACM, 2018.

[20] D. Seo, R. M. Neely, K. Shen, U. Singhal, E. Alon, J. M. Rabaey, J. M. Carmena, and M. M. Maharbiz, "Wireless recording in the peripheral nervous system with ultrasonic neural dust," *Neuron*, vol. 91, no. 3, pp. 529–539, 2016.

[21] Y. Ma, Z. Luo, C. Steiger, G. Traverso, and F. Adib, "Enabling deep-tissue networking for miniature medical devices," in *ACM SIGCOMM*, 2018.

[22] U. Science and T. P. Office, "Nanotechnology-inspired grand challenges for the next decade," *Federal Register*, 2015.

[23] S. Gabriel, R. W. Lau, and C. Gabriel, "The dielectric properties of biological tissues: III. Parametric models for the dielectric spectrum of tissues," *Physics in Medicine & Biology*, vol. 41, no. 11, p. 2271, 1996.

[24] C. A. Balanis, *Antenna theory: analysis and design; 4th ed.* Somerset: Wiley, 2015.

[25] R. Fano, "Theoretical limitations on the broadband matching of arbitrary impedances," *Journal of the Franklin Institute*, vol. 249, no. 2, pp. 139–154, 1950.

[26] J. Kang, S. Rao, P. Chiang, and A. Natarajan, "Design and Optimization of Area-Constrained Wirelessly Powered CMOS UWB SoC for Localization Applications," *IEEE Transactions on Microwave Theory and Techniques*, vol. 64, pp. 1042–1054, April 2016.

[27] P. Zhang, M. Rostami, P. Hu, and D. Ganesan, "Enabling practical backscatter communication for on-body sensors," in *Proceedings of the 2016 ACM SIGCOMM Conference*, pp. 370–383, ACM, 2016.

[28] K. L. Montgomery, A. J. Yeh, J. S. Ho, V. Tsao, S. M. Iyer, L. Grosenick, E. A. Ferenczi, Y. Tanabe, K. Deisseroth, S. L. Delp, *et al.*, "Wirelessly powered, fully internal optogenetics for brain, spinal and peripheral circuits in mice," *Nature methods*, 2015.

[29] The Independent, "Swedish workers implanted with microchips to replace cash cards and ID passes," 2017. https://www.independent.co.uk/news/world/europe/sweden-workers-microchip-implant-cash-card-id-pass-replace-employee-hand-epicenter-rice-grain-size-a7670551.html.

[30] A. S. Poon, S. O'Driscoll, and T. H. Meng, "Optimal frequency for wireless power transmission into dispersive tissue," *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 5, pp. 1739–1750, 2010.

[31] D. Nikolayev, M. Zhadobov, and R. Sauleau, "Impact of tissue electromagnetic properties on radiation performance of in-body antennas," *IEEE Antennas and Wireless Propagation Letters*, vol. 17, no. 8, pp. 1440–1444, 2018.

[32] T. Wei and X. Zhang, "Gyro in the air: tracking 3D orientation of batteryless internet-of-things," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, pp. 55–68, 2016.

[33] M. Rostami, J. Gummeson, A. Kiaghadi, and D. Ganesan, "Polymorphic radios: A new design paradigm for ultra-low power communication," in *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, pp. 446–460, 2018.

[34] S. Naderiparizi, M. Hessar, V. Talla, S. Gollakota, and J. R. Smith, "Towards battery-free HD video streaming," in *15th USENIX Symposium on Networked Systems Design and Implementation NSDI 18)*, pp. 233–247, 2018.

[35] C. J. Panagamuwa, A. Chauraya, and J. C. Vardaxoglou, "Frequency and beam reconfigurable antenna using photoconducting switches," *IEEE Transactions on Antennas and Propagation*, vol. 54, pp. 449–454, Feb 2006.

[36] H. Wong, W. Lin, L. Huitema, and E. Arnaud, "Multi-polarization reconfigurable antenna for wireless biomedical system," *IEEE transactions on biomedical circuits and systems*, vol. 11, no. 3, pp. 652–660, 2017.

[37] A. T. Kolsrud and and, "Dual-frequency electronically tunable CPW-fed CPS dipole antenna," *Electronics Letters*, vol. 34, pp. 609–611, April 1998.

[38] H. Sun, Y.-x. Guo, M. He, and Z. Zhong, "Design of a high-efficiency 2.45-GHz rectenna for low-input-power energy harvesting," *IEEE Antennas and Wireless Propagation Letters*, vol. 11, pp. 929–932, 2012.

[39] A. K. Skrivervik, "Implantable antennas: The challenge of efficiency," in *2013 7th European conference on antennas and propagation (EuCAP)*, pp. 3627–3631, IEEE, 2013.

[40] F. Merli, L. Bolomey, J.-F. Zurcher, G. Corradini, E. Meurville, and A. K. Skrivervik, "Design, realization and measurements of a miniature antenna for implantable wireless communication systems," *IEEE Transactions on Antennas and propagation*, vol. 59, no. 10, pp. 3544–3555, 2011.

[41] A. Y.-S. Jou, H. Pajouhi, R. Azadegan, and S. Mohammadi, "A CMOS integrated rectenna for implantable applications," in *2016 IEEE MTT-S International Microwave Symposium (IMS)*, pp. 1–3, IEEE, 2016.

[42] B. J. DeLong, A. Kiourti, and J. L. Volakis, "A radiating near-field patch rectenna for wireless power transfer to medical implants at 2.4 GHz," *IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology*, vol. 2, no. 1, pp. 64–69, 2018.

[43] R. Lodato, V. Lopresto, R. Pinto, and G. Marrocco, "Numerical and experimental characterization of through-the-body UHF-RFID links for passive tags implanted into human limbs," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 10, pp. 5298–5306, 2014.

[44] C. Liu, Y.-X. Guo, H. Sun, and S. Xiao, "Design and safety considerations of an implantable rectenna for far-field wireless power transfer," *IEEE Transactions on antennas and Propagation*, vol. 62, no. 11, pp. 5798–5806, 2014.

[45] A. Yakovlev, J. H. Jang, and D. Pivonka, "An 11μW Sub-pJ/bit Reconfigurable Transceiver for mm-Sized Wireless Implants," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 10, pp. 175–185, Feb 2016.

[46] P. Zhang, D. Bharadia, K. Joshi, and S. Katti, "HitchHike: Practical Backscatter Using Commodity WiFi," in *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, pp. 259–271, ACM, 2016.

[47] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: wireless communication out of thin air," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 39–50, 2013.

[48] J. Jang and F. Adib, "Underwater backscatter networking," in *Proceedings of the ACM Special Interest Group on Data Communication*, pp. 187–199, 2019.

[49] Z. Pengyu, G. Jeremy, and G. Deepak, "BLINK: a high throughput link layer for backscatter communication," in *Proceedings of the 10th international conference on Mobile systems, applications, and services*, MobiSys '12, (New York, NY, USA), pp. 99–112, ACM, 2012.

[50] G. Wei, C. Si, L. Jiangchuan, and W. Zhi, "MobiRate: Mobility-Aware Rate Adaptation Using PHY Information for Backscatter Networks," in *IEEE Conference on Computer Communications*, INFOCOM'18, (New York, NY, USA), pp. 1259–1267, IEEE, 2018.

[51] L. Vincent, T. Vamsi, and G. Shyanmnath, "Enabling instantaneous feedback with full-duplex backscatter," in *Proceedings of the 20th annual international conference on Mobile computing and networking*, MobiCOM '14, (New York, NY, USA), pp. 67–78, ACM, 2014.

[52] J. Charthad, M. J. Weber, T. C. Chang, and A. Arbabian, "A mm-sized implantable medical device (IMD) with ultrasonic power transfer and a hybrid bi-directional data link," *IEEE Journal of solid-state circuits*, vol. 50, no. 8, pp. 1741–1753, 2015.

[53] Y.-S. Seo, Z. Hughes, D. Isom, M. Q. Nguyen, S. Deb, S. Rao, and J.-C. Chiao, "Wireless power transfer for a miniature gastrostimulator," in *Microwave Conference (EuMC), 2012 42nd European*, pp. 229–232, IEEE, 2012.

[54] J. S. Ho, A. J. Yeh, E. Neofytou, S. Kim, Y. Tanabe, B. Patlolla, R. E. Beygui, and A. S. Poon, "Wireless power transfer to deep-tissue microimplants," *Proceedings of the National Academy of Sciences*, vol. 111, no. 22, pp. 7974–7979, 2014.

[55] A. Aldaoud, C. Laurenson, F. Rivet, M. R. Yuce, and J.-M. Redouté, "Design of a Miniaturized Wireless Blood Pressure Sensing Interface Using Capacitive Coupling," *IEEE/ASME Transactions on Mechatronics*, vol. 20, no. 1, pp. 487–491, 2015.

[56] D. M. Pozar, *Microwave engineering; 3rd ed.* Hoboken, NJ: Wiley, 2005.

[57] J. Kang, P. Y. Chiang, and A. Natarajan, "A 1.2cm^2 2.4GHz self-oscillating rectifier-antenna achieving -34.5dBm sensitivity for wirelessly powered sensors," in *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 374–375, Jan 2016.

[58] C. Dagdeviren, "The future of bionic dynamos," *Science*, vol. 354, no. 6316, pp. 1109–1109, 2016.

[59] Z. Bao, Y. Guo, and R. Mittra, "Single-Layer Dual-/Tri-Band Inverted-F Antennas for Conformal Capsule Type of Applications," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 12, pp. 7257–7265, 2017.

[60] K. R. Sadagopan, J. Kang, Y. Ramadass, and A. Natarajan, "A 960pW Co-Integrated-Antenna Wireless Energy Harvester for WiFi Backchannel Wireless Powering," in *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*, pp. 136–138, Feb 2018.

[61] H. . Son and C. . Pyo, "Design of RFID tag antennas using an inductively coupled feed," *Electronics Letters*, vol. 41, no. 18, pp. 994–996, 2005.

[62] "Avery denison." `http://rfid.averydennison.com`. Avery Denison.

[63] D. Dardari, R. D'Errico, C. Roblin, A. Sibille, and M. Z. Win, "Ultrawide bandwidth RFID: The next generation?," *Proceedings of the IEEE*, vol. 98, no. 9, pp. 1570–1582, 2010.

[64] P. P. Mercier and A. P. Chandrakasan, "Rapid Wireless Capacitor Charging Using a Multi-Tapped Inductively-Coupled Secondary Coil," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, no. 9, pp. 2263–2272, 2013.

[65] M. Stoopman, S. Keyrouz, H. J. Visser, K. Philips, and W. A. Serdijn, "A self-calibrating RF energy harvester generating 1V at −26.3 dBm," in *2013 Symposium on VLSI Circuits*, pp. C226–C227, 2013.

[66] "Ansys HFSS." `https://www.ansys.com/products/electronics/ansys-hfss`. Ansys High Frequency Structure Simulator (HFSS).

[67] "Flexpcb." `https://flexpcb.com/`. FlexPCB.

[68] "EPC UHF Gen2 Air Interface Protocol." `http://www.gs1.org/epcrfid/epc-rfid-uhf-air-interface-protocol/2-0-1`.

[69] "Agilent N9020A MXA Signal Analyzer." `https://www.keysight.com/en/pdx-x202266-pn-N9020A/mxa-signal-analyzer-10-hz-to-265-ghz?cc=US&lc=eng`.

[70] "USRP n210." `http://www.ettus.com`. ettus inc.

[71] "SBX daughterboard." `http://www.ettus.com`. ettus inc.

[72] "LFRX daughterboard." `http://www.ettus.com`. ettus inc.

[73] "CDA2990." `http://www.ettus.com`. Ettus Inc.

[74] "LP0410." `http://www.ettus.com`. Ettus Inc.

[75] "Keysight N5183B MXG Analog Signal Generator." https://www.keysight.com/en/pdx-x202011-pn-N5183B/mxg-x-series-microwave-analog-signal-generator-9-khz-to-40-ghz?cc=US&lc=eng.

[76] Keithley Instruments, Inc., *Model 2400 SourceMeter Instrument*, 10 2018.

[77] C. Dagdeviren, B. D. Yang, Y. Su, P. L. Tran, P. Joe, E. Anderson, J. Xia, V. Doraiswamy, B. Dehdashti, X. Feng, B. Lu, R. Poston, Z. Khalpey, R. Ghaffari, Y. Huang, M. J. Slepian, and J. A. Rogers, "Conformal piezoelectric energy harvesting and storage from motions of the heart, lung, and diaphragm," *Proceedings of the National Academy of Sciences*, vol. 111, no. 5, pp. 1927–1932, 2014.

[78] C. Dagdeviren, F. Javid, P. Joe, T. von Erlach, T. Bensel, Z. Wei, S. Saxton, C. Cleveland, L. Booth, S. McDonnell, J. Collins, A. Hayward, R. Langer, and G. Traverso, "Flexible piezoelectric devices for gastrointestinal motility sensing," *Nature Biomedical Engineering*, vol. 1, no. 10, pp. 807–817, 2017.

[79] M. J. Weber, Y. Yoshihara, A. Sawaby, J. Charthad, T. C. Chang, and A. Arbabian, "A Miniaturized Single-Transducer Implantable Pressure Sensor With Time-Multiplexed Ultrasonic Data and Power Links," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 4, pp. 1089–1101, 2018.

[80] U. Banerjee, A. Wright, C. Juvekar, M. Waller, Arvind, and A. P. Chandrakasan, "An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for Securing Internet-of-Things Applications," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 8, pp. 2339–2352, 2019.

[81] F. Pareschi, G. Setti, and R. Rovatti, "Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 12, pp. 3124–3137, 2010.

[82] M. Kim, U. Ha, Y. Lee, K. Lee, and H.-J. Yoo, "A 82nW chaotic-map true random number generator based on sub-ranging SAR ADC," in *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, pp. 157–160, 2016.

[83] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "16.3 A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS," in *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, pp. 280–281, 2014.

[84] E. Kim, M. Lee, and J.-J. Kim, "8.2 8Mb/s 28Mb/mJ robust true-random-number generator in 65nm CMOS based on differential ring oscillator with feedback resistors," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 144–145, 2017.

[85] "Agilent 8267C PSG Vector Signal Generator." https://www.keysight.com/us/en/product/E8267C/psg-vector-signal-generator.html.

[86] S. Jeong, Y. Kim, G. Kim, and D. Blaauw, "A Pressure Sensing System with ± 0.75 mmHg (3σ) Inaccuracy for Battery-Powered Low Power IoT Applications," in *2020 IEEE Symposium on VLSI Circuits*, pp. 1–2, 2020.

[87] S. Oh, Y. Shi, G. Kim, Y. Kim, T. Kang, S. Jeong, D. Sylvester, and D. Blaauw, "A 2.5nJ duty-cycled bridge-to-digital converter integrated in a 13mm^3 pressure-sensing system," in *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*, pp. 328–330, 2018.

[88] H. Bhamra, J.-W. Tsai, Y.-W. Huang, Q. Yuan, and P. Irazoqui, "21.3 A sub-mm^3 wireless implantable intraocular pressure monitor microsystem," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 356–357, 2017.

[89] NIST, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *NIST Special Publication*, vol. 800-22 Rev. 1a, 2010.

[90] NIST, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," *NIST Special Publication*, vol. 800-38D, 2007.

[91] N. E. Roberts, K. Craig, A. Shrivastava, S. N. Wooters, Y. Shakhsheer, B. H. Calhoun, and D. D. Wentzloff, "A 236nW -56.5dBm-Sensitivity Bluetooth Low-Energy Wakeup Receiver with Energy Harvesting in 65nm CMOS," in *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 450–451, Jan 2016.

[92] M. Ding, P. Zhang, C. Lu, Y. Zhang, S. Traferro, G. van Schaik, Y. Liu, J. Huijts, C. Bachmann, G. Dolmans, and K. Philips, "A 2.4GHz BLE-compliant fully-integrated wakeup receiver for latency-critical IoT applications using a 2-dimensional wakeup pattern in 90nm CMOS," in *2017 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, pp. 168–171, 2017.

[93] H. Jiang, P. P. Wang, L. Gao, P. Sen, Y. Kim, G. M. Rebeiz, D. A. Hall, and P. P. Mercier, "A 4.5nW wake-up radio with -69dBm sensitivity," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 416–417, 2017.

[94] C. Salazar, A. Kaiser, A. Cathelin, and J. Rabaey, "A -97dBm-sensitivity interferer-resilient 2.4GHz wake-up receiver using dual-IF multi-N-Path architecture in 65nm CMOS," in *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, pp. 1–3, Feb 2015.

[95] M. R. Abdelhamid, "Ultra low power, high sensitivity secure wake-up receiver for the Internet of Things (Can be downloaded at http://hdl.handle.net/1721.1/111908)," Master's thesis, Massachusetts Institute of Technology, Cambridge, 2017.

[96] P.-H. P. Wang and P. P. Mercier, "28.2 A 220μW -85dBm Sensitivity BLE-Compliant Wake-up Receiver Achieving -60dB SIR via Single-Die Multi- Channel FBAR-Based Filtering and a 4-Dimentional Wake-Up Signature," in *2019 IEEE International Solid- State Circuits Conference - (ISSCC)*, pp. 440–442, 2019.

[97] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "ORACLE: Optimized Radio clAssification through Convolutional neuraL nEtworks," 2018.

[98] K. Youssef, L.-S. Bouchard, K. Z. Haigh, H. Krovi, J. Silovsky, and C. P. V. Valk, "Machine Learning Approach to RF Transmitter Identification," 2017.

[99] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 160–167, 2018.

[100] "Redbear BLE Nano v2 board." `https://github.com/redbear/nRF5x`.

[101] "Nordic nRF52832: Versatile Bluetooth 5.2 SoC supporting Bluetooth Low Energy, Bluetooth mesh and NFC." `https://www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF52832`.

[102] A. Nourbakhsh, A. Zubair, S. Joglekar, M. Dresselhaus, and T. Palacios, "Subthreshold swing improvement in MoS_2 transistors by the negative-capacitance effect in a ferroelectric Al-doped-HfO_2/HfO_2 gate dielectric stack," *Nanoscale*, vol. 9, pp. 6122–6127, 2017.

[103] X. Zhang, J. Grajal, J. L. Vazquez-Roy, U. Radhakrishna, X. Wang, W. Chern, L. Zhou, Y. Lin, P.-C. Shen, X. Ji, X. Ling, A. Zubair, Y. Zhang, H. Wang, M. Dubey, J. Kong, M. Dresselhaus, and T. Palacios, "Two-dimensional MoS_2-enabled flexible rectenna for Wi-Fi-band wireless energy harvesting," *Nature*, vol. 566, no. 7744, pp. 368–372, 2019.

[104] G. Zhang, H. He, and D. Katabi, "Circuit-GNN: Graph Neural Networks for Distributed Circuit Design," in *Proceedings of the 36th International Conference on Machine Learning*, vol. 97 of *Proceedings of Machine Learning Research*, pp. 7364–7373, PMLR, Jun 2019.

[105] S. Maji, U. Banerjee, S. H. Fuller, M. R. Abdelhamid, P. M. Nadeau, R. T. Yazicigil, and A. P. Chandrakasan, "A Low-Power Dual-Factor Authentication Unit for Secure Implantable Devices," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–4, 2020.

[106] M. I. Ibrahim, M. I. Wasiq Khan, C. S. Juvekar, W. Jung, R. T. Yazicigil, A. P. Chandrakasan, and R. Han, "29.8 THzID: A 1.6mm^2 Package-Less Cryptographic Identification Tag with Backscattering and Beam-Steering at 260GHz," in *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, pp. 454–456, 2020.

[107] Q. Zhou, Y. He, K. Yang, and T. Chi, "12.3 Exploring PUF-Controlled PA Spectral Regrowth for Physical-Layer Identification of IoT Nodes," in *2021 IEEE International Solid- State Circuits Conference (ISSCC)*, vol. 64, pp. 204–206, 2021.