Ultra Low Power, High Sensitivity Secure Wake-up Receiver for the Internet of Things

by

Mohamed Radwan Abdelhamid

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

Master of Science in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2017

Author ..... Signature redacted .....
Department of Electrical Engineering and Computer Science
May 19, 2017

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

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

Ultra Low Power, High Sensitivity Secure Wake-up Receiver for the Internet of Things

by

Mohamed Radwan Abdelhamid

Submitted to the Department of Electrical Engineering and Computer Science
on May 19, 2017, in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering and Computer Science

Abstract

Internet of Things (IoT) is emerging as the technology of the future where an estimate of billions of devices around us will be connected to the internet. When all of these sensors and nodes get connected to the cloud, a huge portion of their energy is consumed by their wireless communication systems. However, most of the sensors and nodes have a highly constrained power budget or even operate using a batteryless energy-harvesting scheme. With tons of data being transmitted through the IoT nodes, the specifications dictate an ultra low power design with secure communication.

An ultra low power wake-up receiver integrated circuit is designed which can wake any node up using Bluetooth-LE. A new system level design methodology is introduced to map the higher level specifications to circuit level requirements with optimized duty cycling. A low power architecture is presented utilizing a mixer-first architecture along with a low power free-running oscillator. The system is designed to be highly programmable in order to track the local oscillator frequency variations through a cascade of reconfigurable filters along the receiver chain. While the whole system is optimized to be duty cycled in a scheme suitable for receiving the Bluetooth LE advertising packets, the local oscillator is also duty-cycled within the short interval of active operation in a harmonic rejection scheme for a 33% further power reduction.

A prototype wake-up receiver with BLE compliance was designed using 65nm CMOS technology. The receiver correlates to a 32-bit reconfigurable wake-up pattern at a -90 dBm sensitivity using the advertising packets only without an actual connection. The system operates from a 0.7 V supply and consumes a 1 μW at a latency of a couple of seconds through incorporating an optimized system level duty cycling and within-bit duty cycling schemes. The power consumption can be be further scaled down to 400 nW or less at a latency of ten seconds or greater making it suitable for low power and low datarate IoT transceivers.

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

Acknowledgments

I would like to thank Professor Anantha Chandrakasan for giving me the opportunity to join his research group. It was a great honor to be working with him. I would like to thank him for guiding me from the very beginning on picking a topic to work on and always providing me with new interesting research directions along the way.

I would like to also thank Arun for his great help starting with all of those brainstorming meetings all the way to the tips in simulations and layout. Also, thanks for your guidance and advice even remotely after you have graduated.

I'd like to thank Utsav and Taehoon for all of our chats and adventure in our first year here at MIT. Also, for their help in the courses we took together.

I have to thank all the members of Anantha group where I can always find the answer to any question I have. I always loved our gatherings and even more our little circles. I'd like to especially thank Phil for all of his help in the tapeout and the testing setup. And a special thanks goes to Margaret for being such a great help to the whole team with such a meticulous coordination.

I definitely would like to thank our little Boston gang starting with my roommate Qasim for being there for me from the start of our first week here up till now. I want to also thank the rest of the gang Malik, Amira, Mahmoud, Mustafa, Sally and Ibrahim for our hangouts and competitive squash tournaments. Also, Shahd and Eddy for our great outings.

I want to thank my friends back in Egypt Karim, Hossam, M. Kamel, and my twin brother Mostafa for their constant motivation. They always cheered me up whenever I needed it.

And of course all of this has to be dedicated to my family. My parents have always encouraged me to pursue my dreams and to work hard to reach my goals. They are the reason I got all the way here. I want to thank my brother Ahmed for always checking on me and my sisters Reem and Salma for their support and their kids for just being those little bundles of joy they are.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background and Motivation

The future holds a world where everything will be connected to the internet, no matter how big or small it was, through the so called Internet of Things or the IoT. As the name implies, all things around us will be connected to the internet. With such ubiquitous connectivity, all kinds of daily tasks will become only one keystroke away. For instance, in a not so distant future, the home appliances will update the owner with the needed groceries or even order them online on a weekly basis with a simple user authentication. More importantly, an always-connected security system will facilitate monitoring and tracking of infants.

Another field that has been undergoing a steady revolutionizing development through the IoT is the biomedical industry. Non invasive biomedical measurements have become possible with the use of in body sensors that can communicate directly to the patient's cellphone as well as to the doctor's. Such IoT devices not only monitor the patients and update an electronic health record but can also interfere and provide some sort of remotely controlled drug delivery. For example, a diabetic patient can have a glucose measurement sensor that automatically injects insulin in the blood

stream through an automated closed system or with a simple manual command using a smart phone.

Initially, IoT devices estimates started with an explosive estimate of trillion of devices to be connected to the internet by 2020. However, this overestimation changed with time till it settled on a more realistic estimate of the number of IoT devices. Such estimate is reported by several companies including *IHS Markit* which reports a current value of about 20 Billion devices as shown in Figure 1-1 and is expected to grow to about 75 Billions by the year 2025 [1].

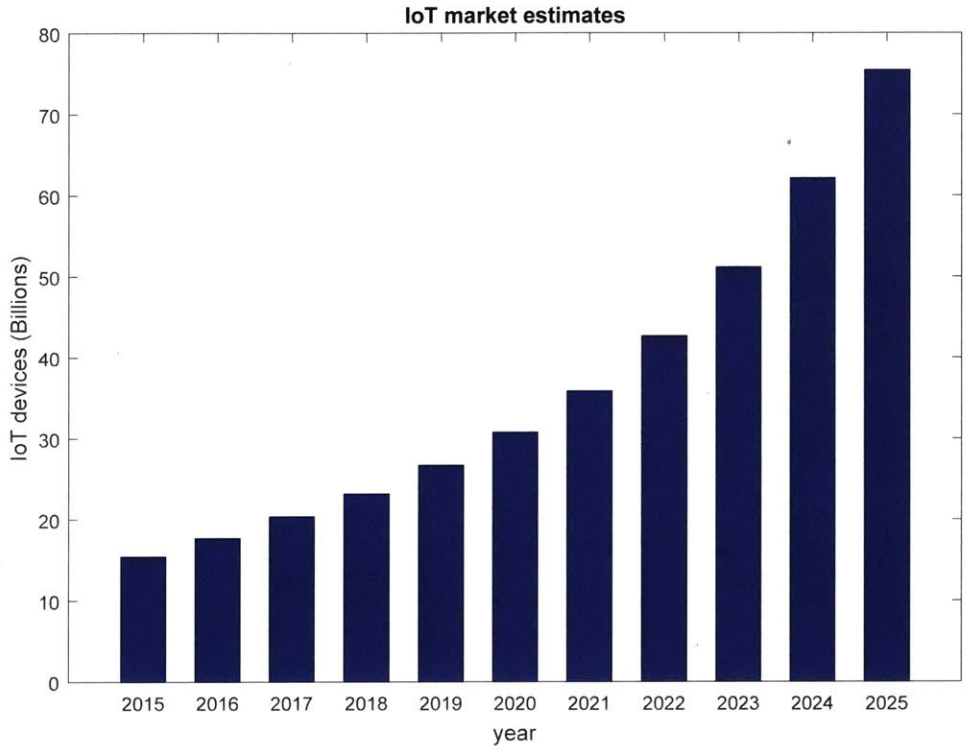


Figure 1-1: IHS estimate of IoT devices in the next ten years

1.1.1 IoT Transceivers constraints

A conventional IoT network is shown in Figure 1-2 where different nodes are connected to the cloud. For all kinds of sensors and nodes to be connected, then they need some sort of wireless communication circuitry just like the smartphones and laptops.

Unfortunately, these IoT nodes consume a huge portion of their energy on their wireless systems. While the smartphones and laptops can be easily charged whenever their battery gets drained, the ubiquitous IoT devices on the other hand are not as accessible. An IoT network could be composed of devices widespread in an industrial manufacturing environment or even of some sensors in a human body. In other words, charging an IoT node or replacing its battery is usually not an easy task and might even require a surgery with all the risks associated with it. Hence, these nodes need to operate with a very tight power budget or even in an energy-harvesting environment so that it can last for tens of years without battery replacement.

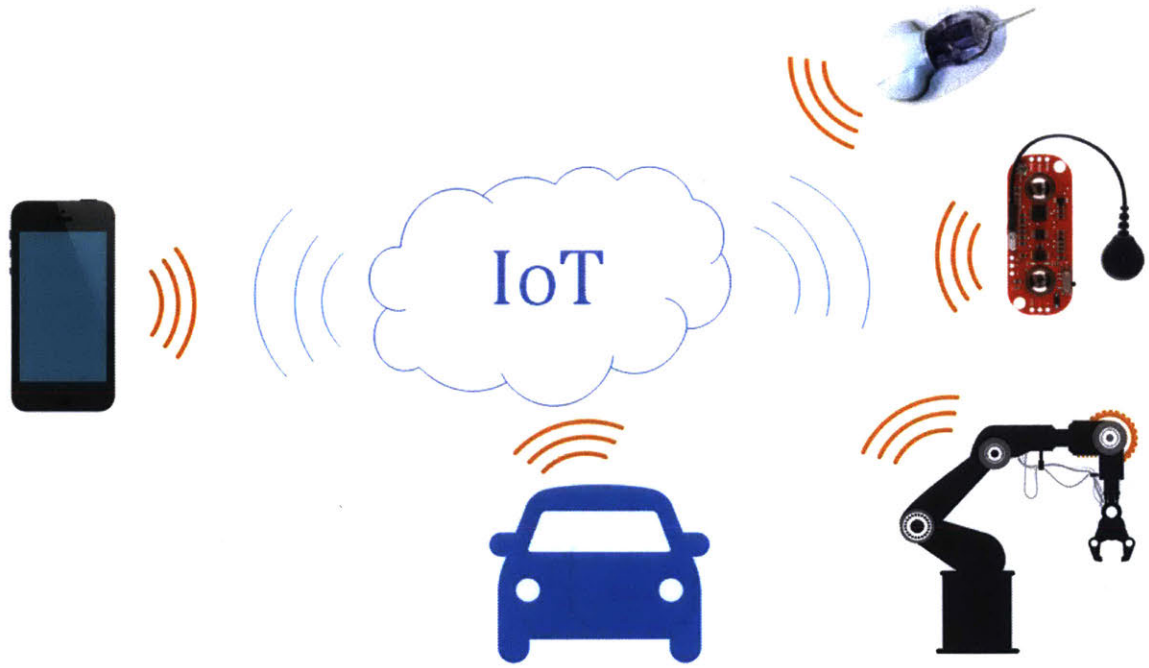


Figure 1-2: A network of IoT devices

1.2 Communication standards limits and potentials

Several communications standards exist in the literature and are even well established in their markets such as WiFi, 4G, Bluetooth LE, MICS, Zigbee, ... etc. However, the

IoT market hasn't really settled on a specific standard for all of its devices. The ultra-low power demand has often been a much stronger driving force than the convenience of complying with a pre-existing standard.

Several techniques can be employed to achieve ultra low power consumption. One of which is heavy duty cycling where the IoT node is asleep for the majority of time in an ultra low power mode and is only active in the high power mode for a short interval reducing the average power consumption. As illustrated in [2], in order to communicate with the sleeping node, either a protocol-based duty-cycling or an on demand wake-up can be used. In the protocol-based dutycycling, a global clock synchronizes the periodic wake-up time with the user's transmission to guarantee reception with fixed power savings. On the other hand, on demand wake-up uses an interface circuit, called the wake-up receiver, which decodes the user's wake-up request and produce a wake-up signal to the sleeping node as shown in Figure 1-3. Then, the IoT node becomes active and the user's base station transmission is initiated. Hence, the node can sleep at its lowest possible power as long as the user doesn't need to wake it up.

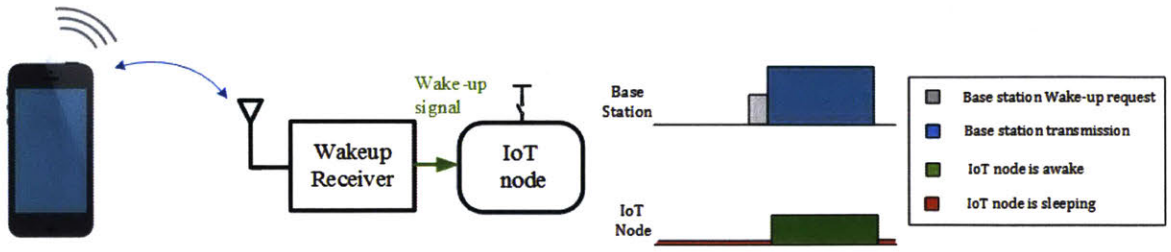


Figure 1-3: Wake-up receivers for IoT nodes

Many of the IoT wake-up receivers employ an OOK (On-Off keying) modulation scheme due to its simplicity and low power consumption yet its spectral inefficiency deems it unsuitable for most wireless standards. For instance, the work in [3] describes a low-voltage low-power wake-up receiver achieving a sensitivity as good as -97 dBm for an OOK receiver at 2.4 GHz without complying with an existing standard.

1.2.1 Bluetooth LE Potential

Coming up as the most energy efficient wireless communication standard, Bluetooth Low Energy (BLE) serves as the best candidate for IoT applications. In addition to its efficiency, it provides such a convenient communication process due to its availability in smart phones and laptops. Hence, a user can easily communicate with an IoT node without the need of a special router that acts as a liaison between a standard wireless network and a non-standardized IoT network.

A commercial off the shelf Bluetooth LE transceiver chip was analyzed in [4] to determine the power consumption limits at different duty cycles. It models the average power consumption of a commercial +10 dBm BLE chip as [5] by breaking it down to active power constituents and stand-by power portion. Such a model is described as

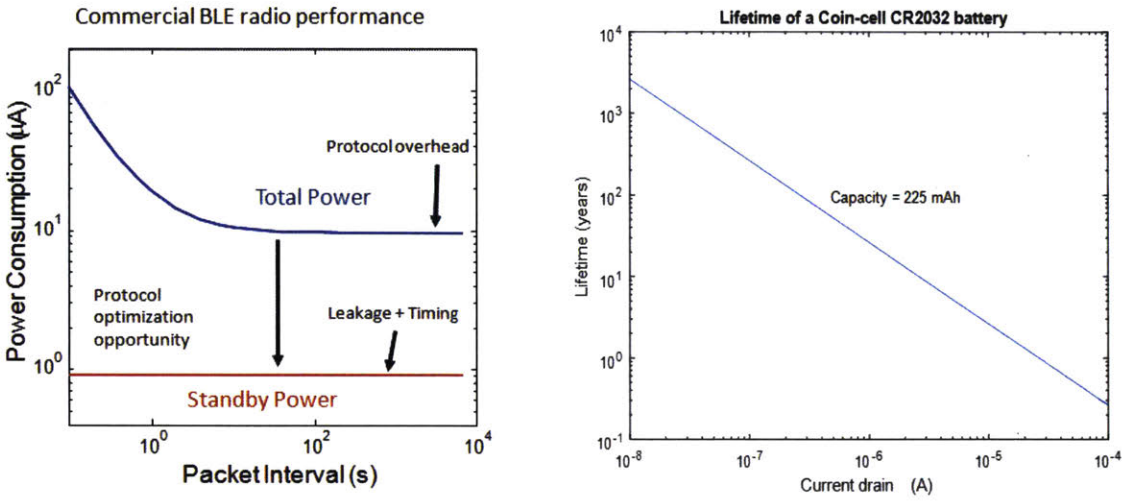
$$P_{avg} = \frac{T_{comm}}{T_{Duty}} \cdot P_{ON} + \frac{T_{overhead}}{T_{Duty}} \cdot P_{ON} + \left(1 - \frac{T_{comm}}{T_{Duty}} - \frac{T_{overhead}}{T_{Duty}}\right) \cdot P_{sleep} \qquad (1.1)$$

where T_{comm} is the time required for BLE packets communication during a connection, T_{Duty} is the duty-cycling interval of the system, $T_{overhead}$ is the interval in which the radios are active due to the protocol overhead to maintain the connection, P_{ON} is the active power consumption when the radio is ON while P_{sleep} is the stand-by power during sleep-mode.

As shown in Figure 1-4a, the analysis of the commercial BLE chip done in [4] indicates that the power consumption with an active connection is actually limited to tens of microamps. Unfortunately, using a conventional coin cell battery with a capacity of 225 mAh as in [6] would only last a couple of years. At a consumption of 10 μA, such battery capacity will have a lifetime of

$$T = \frac{Capacity}{Current} = \frac{225}{10 \times 10^{-3}} = 22500\ h = 2.57\ years \qquad (1.2)$$

and the general lifetime as a function of current is plotted in Figure 1-4b.



(a) BLE power consumption (b) Commercial battery lifetime

Figure 1-4: BLE limits and potential

Hence, new circuit techniques and optimized communication protocols need to be investigated to mitigate the overhead issues and reach an average consumption around the few microwatts stand-by power range or even less.

1.3 Wake-up Receiver specifications

- **Standard:** In order to be able to wake the node up using handheld devices such as the cell phones or even the laptops, the receiver needs to comply to existing standards. The most convenient and energy efficient one is BLE.

- **Power consumption:** as mentioned in the previous sections, specifically in equation (1.2), an average power consumption below 1 μW is targeted so that the IoT node can last for years without performance degradation or battery replacement.

- **Sensitivity:** BLE standard requires a sensitivity better than -70 dBm and this work targets to break the low-range limitation through a highly sensitive receiver

design of a -90 dBm sensitivity.

- **Data rate:** the datarate depends mainly on the application and the main advantage here is that most IoT applications require a very low rate with a sort of infrequent transmissions. Hence, lower datarates can be utilized for lower power consumption.

- **Modulation scheme:** OOK is a good candidate for low power but the wireless standards compliance dictates the design of a receiver that can demodulate other schemes such as GFSK for Bluetooth-LE.

- **Supply Voltage:** by lowering the supply voltage, lower power consumption can be achieved. This work targets to operate somewhere in the range of voltages below 1 V for lower power with good performance.

- **Security:** an IoT node is vulnerable to battery drainage attacks that further tightens the power consumption limitations. For instance, an adversary node which manages to acquire the wake-up sequence can keep waking the IoT node up draining its battery indefinitely. In this work, the target is to design a more secure system which offers some sort of protection against these kind of attacks.

Table 1.1 summarizes the target specifications for the wake-up receiver.

System specification	
Voltage (V)	< 1
Sensitivity (dBm)	-90
Datarate (kbps)	30 - 300
Average Power (μW)	< 1
Modulation Scheme	GFSK
Wireless Standard	BLE

Table 1.1: Target system level specifications

1.4 Thesis Contributions

1. This thesis presents a new receiver architecture that demodulates a GFSK signal and search for a given wake-up sequence inside the packet to wake the IoT node up. A 0.7 V wake-up receiver prototype is demonstrated at the 2.4 GHz ISM band.

2. BLE compliance is satisfied by embedding the wake-up sequence inside the advertising packets of any BLE advertising device.

3. System-level duty cycling is implemented in an optimized wake-up scheme to achieve sub-μW power consumption at a sensitivity as good as -90 dBm.

4. Within-bit duty-cycling with harmonic cancellation is incorporated in the local oscillator achieving an active power reduction of about 33%.

5. A one-time wake-up pattern is utilized with an event-based pattern update to offer an overall improved system security.

1.5 Thesis Outline

This thesis presents the design of an ultra low power wake-up receiver that can wake up any sensor node using BLE packets in a scheme optimized for the low power Internet of Things. Chapter 2 offers a system level analysis and design methodology to transform the top-level specifications into circuit-level requirements. Chapter 3 provides a survey for existing wake-up receivers with potential improvements. Chapter 4 dives into the circuit-level implementation of the various blocks of the receiver system. Chapter 5 discusses the system optimization for an energy efficient wake-up scheme for Bluetooth Low Energy transmission with improved system security. Finally, chapter 6 provides a conclusion for this work while pointing out potential improvements.

Chapter 2

Ultra Low Power Duty-cycled Transceivers Analysis

In this chapter, a new system level analysis and design methodology is presented which maps the higher level system specifications into circuit level parameters to achieve the required average power consumption under the given system constraints.

2.1 Challenges in Low-Power Transceiver Design

Designing an ultra low power transceiver is definitely not a trivial task as it involves optimization in both the circuit-level design as well as the system-level implementation. To break down the power-performance trade-off, usually the transceiver employs some sort of duty cycling scheme in order to achieve high performance specifications while consuming an ultra low average power.

2.1.1 Duty cycled IoT model

A generic duty cycled transceiver is shown in Figure 2-1 where latency is traded-off with power consumption through duty cycling. This provides a sleep mode for the

transceiver to enter whenever it is not needed or no communication is in process. However, the power-latency trade off must be analyzed and it is critical in the design process to understand what any system level optimization translates to in terms of the circuit-level parameters.

In this model, the base station is treated as a transceiver with an abundant supply of power that can operate continuously for long time intervals which is the case for routers or cell phones. On the other hand, the IoT transceiver is a power-constrained system that is duty cycled such that the active time is much less than the sleep time. The IoT node wake-up can be dictated by the node itself, but will suffer from higher latency. Alternatively, a wake-up receiver in the IoT device can improve the base-station to IoT latency. This thesis explores the design of such wake-up receivers. A duty-cycling approach is considered even for the wake-up receivers themselves, to trade-off latency, and average power.

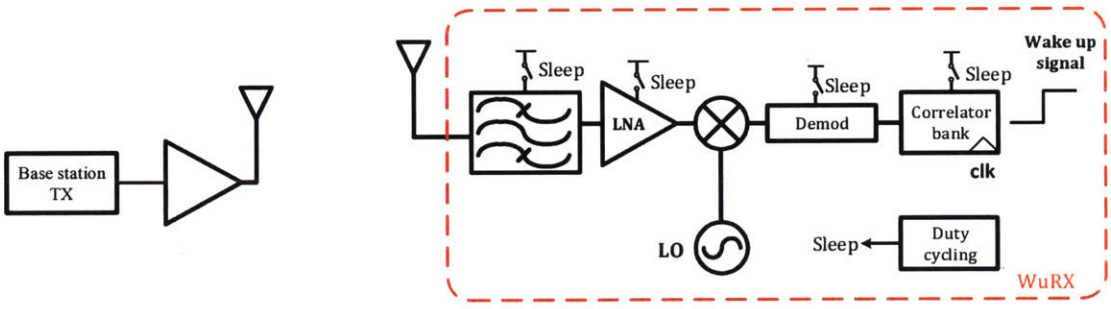


Figure 2-1: A duty cycled transceiver system

The timing diagram for such duty cycling scheme is shown in Figure 2-2 where the Base station transmitter (TX) is active for an ON time of TX_{ON} retransmitting the wake-up packets continuously. In contrast, the wake-up receiver is active for the duration of only two packets in order to guarantee correct reception of one complete packet. In addition to that, it's duty cycled with a period at most equal to the transmitter ON time as well to make sure an overlap occurs between the base station and the IoT node. Hence, the average power consumption is reduced by the ratio

between the active time and the sleep time while the worst case latency is limited by the duty-cycling interval (TX_{ON}) which occurs when the base station starts transmission just after the instant the wake-up receiver enters the sleep mode. This model assumes that the node and the base station are not synchronized. Hence, there is no constraint on the accuracy of the duty-cycling clock leading to potential power savings.

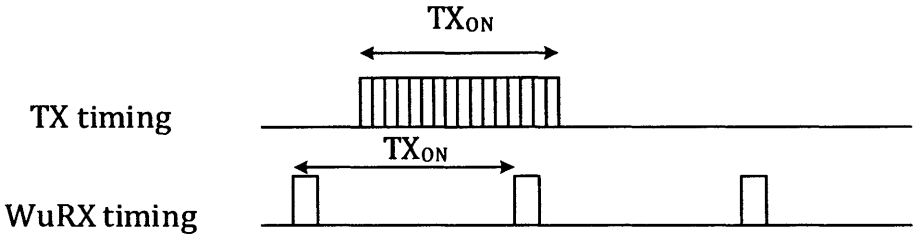


Figure 2-2: Duty-cycling scheme of a wake-up receiver

2.1.2 System level specifications

This section defines the system level specifications and provides the values used throughout the analysis.

- **False alarm rate (FAR):** The rate at which the receiver falsely detects a wake-up packet due to noise, in band interferers, or wake-up packets meant for other nodes.
- **Probability of Detection (P_{det}):** The probability of correctly detecting all bits of the wake-up sequence in the packet.
- **Receiver Active Time (RX_{ON}):** The interval in which the receiver is active and consuming the highest amount of power which directly affects the average power consumption. Within each duty-cycle period, this would be the duration of two wake-up packets.
- **Receiver Sensitivity (P_{sens}):** The minimum detectable signal by the receiver in the band of interest. This sets the maximum range of communication.

In this analysis, the assumed specifications are defined in Table 2.1:

IoT specification	Value
FAR	1 $alarm/hour$
P_{det}	95 %
RX_{ON}	2 $PacketLength$
P_{sens}	-100 dBm

Table 2.1: IoT node system level specifications

2.1.3 Design parameters

With complying to the previously stated system specifications, there are still some design parameters to be explored in the transceiver design space.

- **Receiver Average Power (P_{avg}):** The average power consumed by the receiver might depend on the application, however, an average of hundreds of nanowatts would mean that the node can last for tens of years using conventional batteries.
- **Datarate (DR):** The transmission datarate in IoT tend to be infrequent and usually with small payloads.
- **Duty-cycling period (TX_{ON}):** How often the receiver is duty-cycled directly impacts the system latency as well as the average power consumption.
- **Packet Length (L_{PKT}):** The packet length determines the size of the wake-up sequence. A longer sequence means higher latency while a short sequence has a higher probability of false alarms.

2.1.4 Model equations

By using the model shown in Figure 2-1 and the specifications set by Table 2.1, the required system parameters can be derived for any given average power consumption

P_{avg}. So, in this model, the average power is set to be $P_{avg} = 100\ nW$ while the different design points are generated from different datarates and duty cycling intervals.

First, the FAR determines the packet length for a given duty cycling period.

$$FAR = \frac{False\ Alarms}{Period} = \frac{P(correct\ sequence) \cdot sequences/transmission}{TX_{ON}} \tag{2.1}$$

where a correct sequence occurs only if each bit is correct assuming the bits are independent and random [1]. Hence, each bit has a 50% probability of being '1' or '0'.

$$\therefore P(correct\ sequence) = \overbrace{(\frac{1}{2})(\frac{1}{2})\cdots(\frac{1}{2})}^{L_{PKT}} = \frac{1}{2^{L_{PKT}}} \tag{2.2}$$

and if the receiver is active for a duration of α packets then it can correlate with any consecutive L_{PKT} bits within these packets.

$$sequences/transmission = Total\ bits - L_{PKT} + 1 = \alpha L_{PKT} - L_{PKT} + 1 \tag{2.3}$$

$$\therefore FAR = \frac{1}{2^{L_{PKT}}} \cdot [L_{PKT}(\alpha - 1) + 1] \cdot \frac{1}{TX_{ON}} \tag{2.4}$$

Then, the probability of detection along with the packet length defines the bit error rate (BER) which in turn puts a limit on the required Signal to Noise ratio (SNR). Once these parameters are known, then the circuit noise figure can be calculated in a noise floor of $kT = -174\ dBm/Hz$ as follows:

$$P_{det} = (1 - BER)^{L_{PKT}} \tag{2.5}$$

$$BER = \frac{1}{2} erfc(\sqrt{SNR}) \tag{2.6}$$

$$NF \leq P_{sens} + 174 - 10\ log(DR) - SNR \tag{2.7}$$

[1] Assuming the detection threshold=L_{PKT} which can be improved with a correlator.

The average power consumption then depends linearly on the active power as well as the ratio of active time and can be calculated as follows:

$$P_{avg} = P_{ON} \cdot \frac{RX_{ON}}{TX_{ON}} = P_{ON} \cdot \frac{\alpha L_{PKT}}{TX_{ON} \cdot DR} \tag{2.8}$$

In order to explore the transceiver design space, multiple system models are analyzed for datarates swept over the range [1 $kbps$ – 3 $Mbps$] while the duty-cycling period varies from 30 ms to 30 s which is the range of maximum latencies for the wake-up. Then, for a fixed average power consumption, the active receiver power (P_{ON}) is computed along with the required effective noise figure of the whole receiver chain (NF). Previous work of ultra low power receivers in [2, 7–22] is overlaid on the model with estimates of average power and noise figure for each reference. The output design space is shown in Figure 2-3 showing the different duty-cycling periods and datarates used in each iteration.

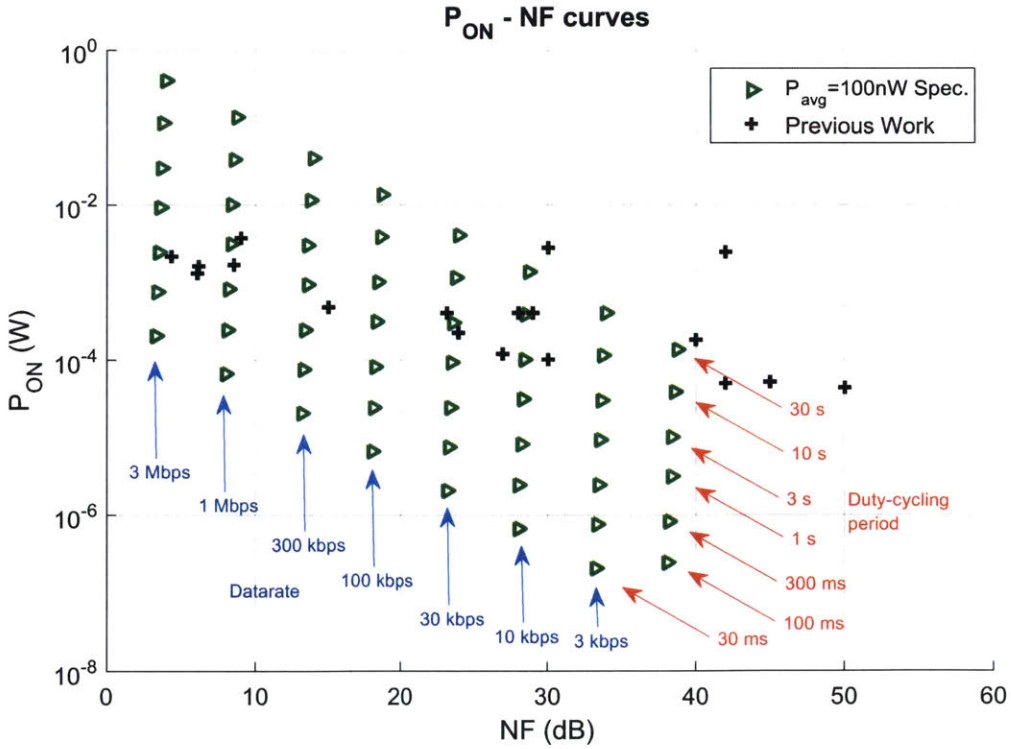


Figure 2-3: Active power and noise figure design space

2.1.5 Constant transmission energy scheme

By analyzing the model at $P_{avg} = 100\ nW$, some trends become clearly visible in the model space. For instance, all systems which have the same transmission energy lie on the same line as shown in Figure 2-4. Hence, if in a system where the base station transmission is restricted to a certain power (e.g. 0 dBm) and can transmit continuously for a maximum of 100 ms, then this transmission might reach the IoT node at a $-100\ dBm$ level carrying a total energy of $E_{in} = P_{in}TX_{ON} = 10fJ$. In consequence, by using the generated design-space plot, a design point can be chosen according to the available input energy to the node.

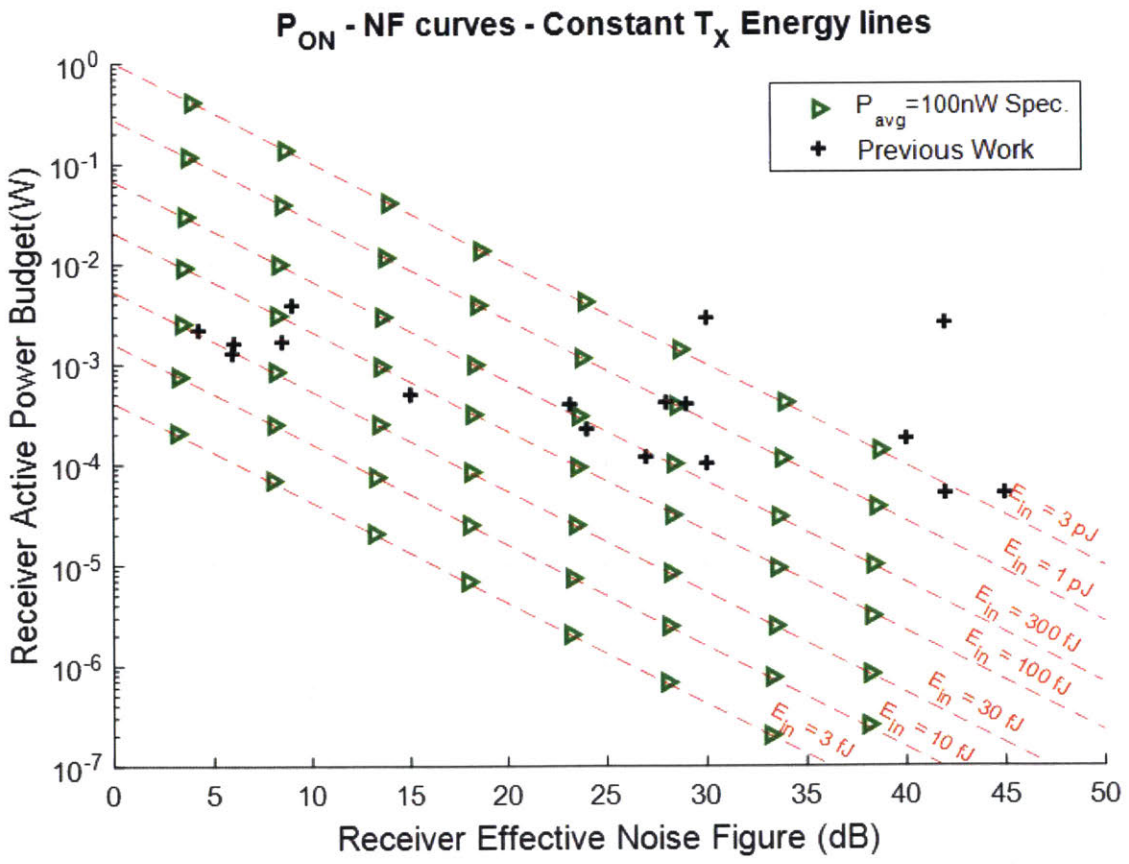


Figure 2-4: Curves of constant transmission energy

2.1.6 Constant bandwidth utilization scheme

One other aspect of concern in highly congested IoT networks is the bandwidth (BW) utilization. A very high duty-cycling period for the IoT node requires the base station to transmit for a very long time in order to guarantee at least one full packet reception. However, this means that the base station occupies a certain BW for long intervals of time which is even worse at higher data rates which translates into bigger BW. The bandwidth utilization is define here as

$$U = DR \cdot TX_{ON} \tag{2.9}$$

As shown in Figure 2-5, the design points which utilize the same BW lie on the same line of constant BW utilization for different data rates. Then for instance,

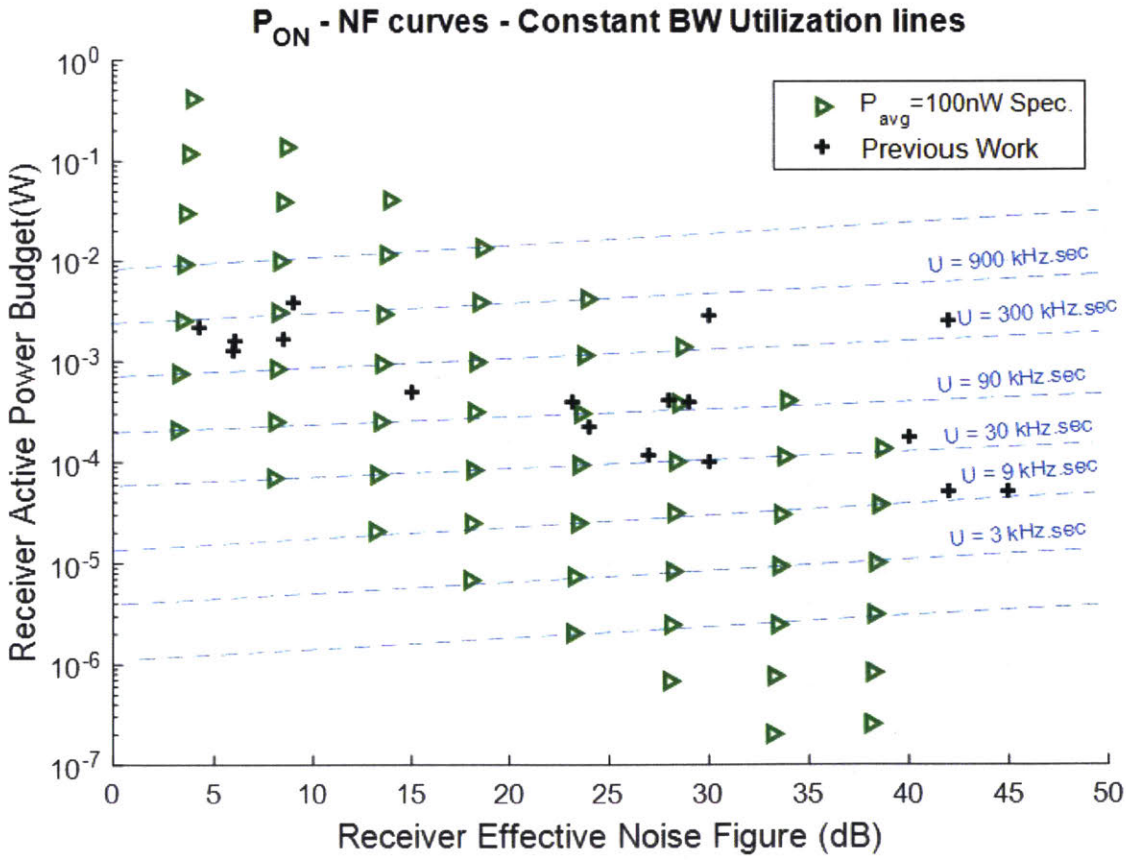


Figure 2-5: Curves of constant BW utilization

if a compromise between bandwidth utilization and transmission energy is to be designed, then as shown in Figure 2-6, a design point can be chosen for example to consume 30 fJ with a utilization of 9 $kHz.sec$. With this point, the rest of the system parameters are then extracted from the model as shown in Table 2.2 and that would be an aggressive improvement over the state of the art as it improves on multiple specifications.

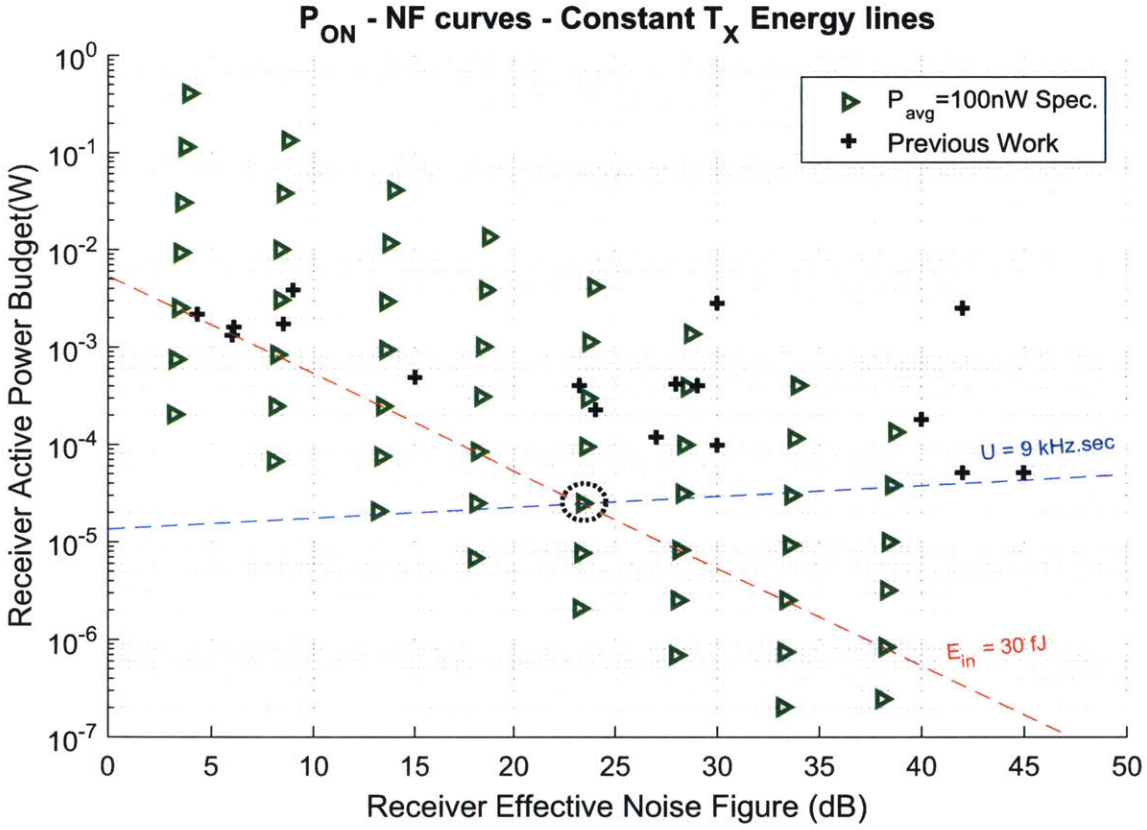


Figure 2-6: A design point for energy-utilization compromise

A couple of trade-offs should be taken into consideration when choosing a design point. For example, the rightmost design points have the lowest datarate of 1 kHz which means that the system should have a center frequency with an accuracy much better than this number, this can be impractical at such low levels of power. On the other hand, the leftmost design points have the highest rates and the startup time of

their oscillators will be more critical.

Model specification	Value
P_{ON}	25 μW
NF	24 dB
DR	30 $kbps$
TX_{ON}	300 ms
E_{in}	30 fJ
L_{PKT}	18 $bits$
P_{sens}	-100 dBm
P_{avg}	100 nW

Table 2.2: Model specifications of the compromise design

2.2 Conclusion

In this chapter, a new methodology for analyzing duty-cycled transceivers is presented where a model for the IoT node is used to estimate the required noise figure and active power for any given system specifications. The model lets the node be duty-cycled while the base station transmits its wake-up request continuously. By fixing the average power consumption, different design points at different datarates can be investigated to reach an optimum design.

Different trade-offs are explored such as the bandwidth utilization as well as the transmission energy and how a compromise between the two extremes can be chosen. Such design point consumes an average power of only 100 nW while the required transmission energy is 30 fJ at a bandwidth utilization of 9 $kHz.sec$. The model then uses these values to predict the circuit level requirements to be an active power of 25 μW at a noise figure of 24 dB and operating at a data rate of 30 kbps.

2.3 Acknowledgment

I want to thank Arun Paidimarri for his help throughout the work in this chapter starting with the node model and equations and providing insight for the different sweeps and choosing a point in the design space.

Chapter 3

Wake-up Receiver Architectures

This chapter presents a literature survey of existing wake-up receiver architectures and then builds on it to develop a new architecture for the proposed receiver.

3.1 Low power architectures

For ultra low power wake-up receiver architectures, there is no standard system or block diagram to follow. Usually, such low power comes at the expense of some performance metric. Hence, the IoT receiver architecture is application dependent where certain blocks of an equivalent high performance receiver are dropped according to the system-level requirements. Some of these architectures are explored in this section to find the most suitable architecture for the required sub-μW wake-up receiver.

Table 3.1 lists a survey of some of the existing wake-up receivers. It is clear that there is almost two different trends. One targets a high sensitivity design with around a hundred microwatts or more while the other direction aims at a lower power consumption of almost hundreds of nanowatts at the expense of sensitivity. The work in [12] uses an unlocked oscillator with dual IF and cascaded filtering to achieve the high sensitivity for the OOK signal. The systems in [8] and [23] utilize an energy detection architecture for an energy efficient OOK demodulation. On the other hand,

a receiver-based frequency locked loop is incorporated in [13] for a sensitivity as good as $-83\ dBm$ at 227 μW.

Specification	[12]	[8]	[23]	[13]
Architecture	Unlocked LO	Energy Detection	Energy Detection	Low-IF
V_{DD} (V)	0.5	0.5/1.2	0.5/1.0	0.6
Sensitivity (dBm)	-97	-45	-39/-56	-83
Average Power	100 μW	116 nW	104/236 nW	227
Frequency (GHz)	2.4	0.403/0.915/2.4	0.4 - 2.4	2.4
Modulation	OOK	OOK	BLE/CDMA	OOK
Technology	65 nm	130 nm	65 nm	65 nm

Table 3.1: Wake-up receiver survey

3.1.1 Energy Detection architecture

One of the most common architectures is the energy detection or the envelope-detector based architecture due to the high simplicity of its architecture, shown in Figure 3-1. Such simple architecture can achieve a power consumption as low as hundreds of nanowatts, however, the energy detection scheme dictates the use of OOK modulation scheme in communication which might not be suitable for a number of applications. Low power comes at the expense of sensitivity, for instance, the designs in [7, 8, 23] achieve hundreds of nanowatts while the work in [24] consumes 4.5 μW but are still all limited in sensitivity to around $-50\ dBm$.

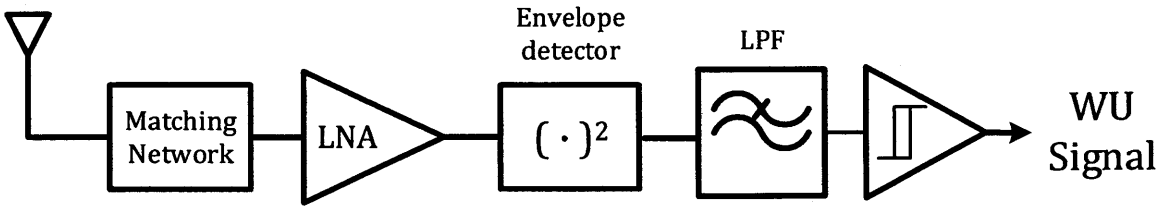


Figure 3-1: Energy-detection architecture block diagram

3.1.2 Injection-locking receiver architecture

As the envelope detector architectures are limited to OOK signals detection, new architectures have been developed to convert Frequency Shift Keying (FSK) signals into OOK signals in order to take advantage of the simple envelope detector circuitry. As shown in Figure 3-2, it utilizes an injection locking oscillator (ILO) whose envelope depends on the frequency of the input. It produces a constant envelope when injected with a signal whose frequency is in the locking range of the oscillator while a frequency outside of this range causes injection pulling which results in a time-varying phase causing an amplitude modulated envelope as shown in Figure 3-3.

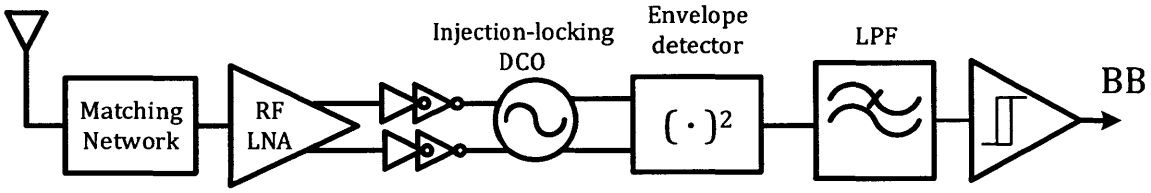


Figure 3-2: Injection-Locking architecture block diagram

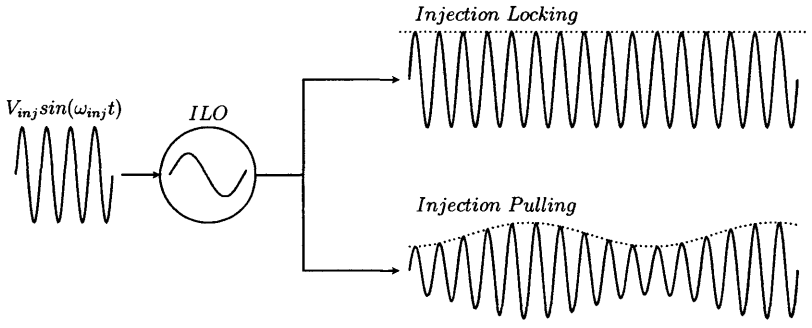


Figure 3-3: Injection locking and pulling waveforms

Such architecture was used in [25] to achieve $-62\ dBm$ sensitivity at a consumption of 45 μW while the work in [26] gets a sensitivity as good as $-87\ dBm$ but a power consumption of 640 μW.

3.1.3 PLL/FLL-based receiver architecture

Processing the input signal directly at radio frequency (RF) incurs high power consumption. Several architectures adopt a phase locked loop (PLL) from the high performance systems or even just a less stringent frequency locked loop (FLL) to generate an accurate oscillator frequency to move all the signal processing to intermediate frequency (IF).

A full high performance PLL consumes almost a 1 mW of power [27] which wouldn't be suitable for the sub-μW receiver budget. A simpler FLL can be used as in [13] which adjusts the system center frequency at a consumption of 227 μW while achieving a receiver sensitivity of -83 dBm. Such architecture is demonstrated in Figure 3-4 where the received OOK signal is down-converted to IF then fed back to the frequency loop to adjust the Voltage Controlled Oscillator (VCO) frequency.

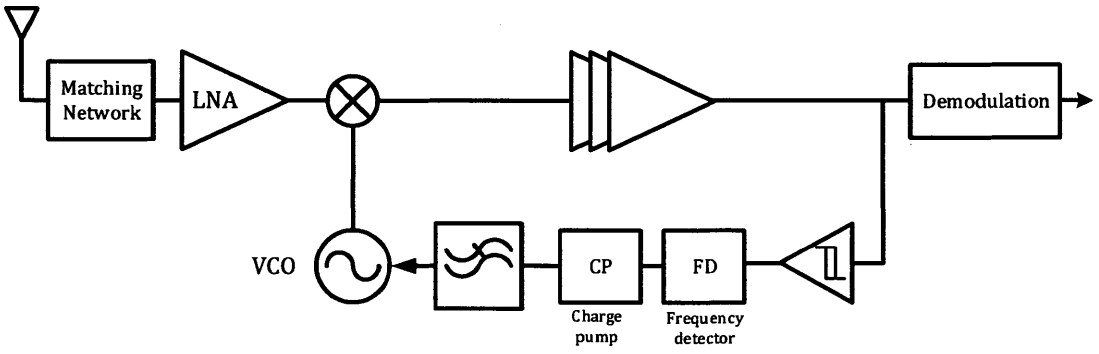


Figure 3-4: OOK receiver utilizing a Receiver-based FLL

3.1.4 Uncertain IF architecture

Uncertain IF architectures exploit the same advantage of the phase or frequency locked loops by moving the signal amplification and processing to a somewhat uncertain IF using only free running oscillators. Then, a wideband envelope detector can be used to convert the signal to a baseband (BB) output as shown in Figure 3-5.

The main issue with this architecture is the uncertainty in its center frequency due to running the oscillator freely without a control loop, this requires wideband IF processing to guarantee capturing the signal in the system's band as shown in Figure 3-6 which can be as high as 100 MHz as in [2]. In consequence, this wide bandwidth takes in a higher amount of thermal noise which degrades the overall sensitivity especially if the RF LNA isn't good enough.

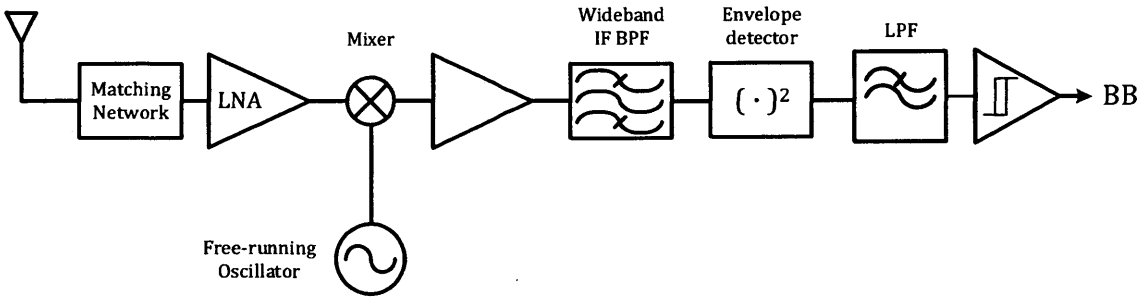


Figure 3-5: Uncertain-IF architecture block diagram

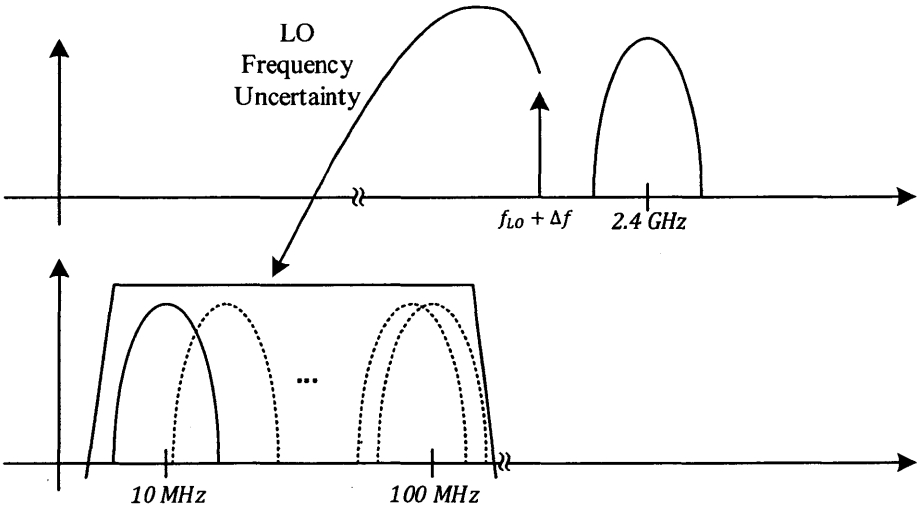


Figure 3-6: Uncertainty in the system Intermediate Frequency (IF)

3.2 Low power RF front-end design

The front-end or the very first block of a receiver defines its performance. For instance, the sensitivity is determined by the noise performance of the chain which is limited by the first stage noise figure and gain. As the noise figure of a chain of N cascaded blocks is given by Friis formula:

$$NF_{tot} = NF_1 + \frac{NF_2 - 1}{G_1} + \frac{NF_2 - 1}{G_1 G_2} + \cdots + \frac{NF_N - 1}{G_1 G_2 \cdots G_{N-1}} \tag{3.1}$$

Hence, there is always a trade-off here between having a low-noise power-hungry first stage such as an RF low noise amplifier (LNA) or on the other hand having an ultra-low power first block with a much higher noise figure and try to adjust the effective noise figure of the whole chain to achieve the required sensitivity.

3.2.1 Direct Energy Detection front-end

Some energy detection architectures use an envelope detector or a rectifier directly as their first stage after the matching network as shown in Figure 3-7. By using the analysis performed in [28] which derives the receiver's sensitivity of an envelope detection receiver as:

$$P_{sens} = 2K_B T \cdot \sqrt{BW_{RF} \cdot BW_{BB} \cdot SNR_{min}} \tag{3.2}$$

where $K_B T$ is the thermal noise floor, BW_{RF} is the RF bandwidth at the input of the envelope detector, BW_{BB} is the baseband bandwidth at its output, and SNR_{min} is the minimum Signal to Noise ratio for a required Bit error rate (BER).

Since the conventional matching networks offer a wide RF bandwidth, then as derived in equation (3.2) this type of energy detection architecture is expected to have

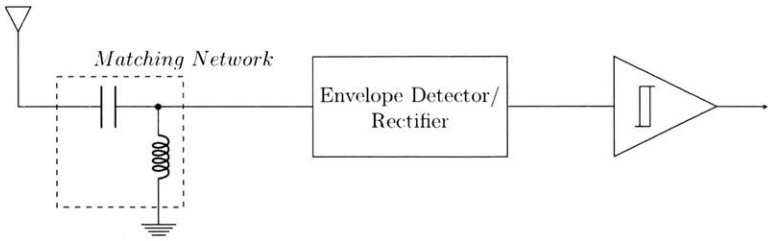


Figure 3-7: Envelope detector as a front-end

low sensitivity and low datarates as in [7]. A correlator can be used at the end of the chain with a re-configurable threshold to get the maximum sensitivity improvement at an acceptable false alarm rate as in [8]. In addition, only a selected node can be chosen to wake-up in a network of multiple IoT nodes.

3.2.2 LNA-first front-end

Adopting from the high performance architectures, several receivers utilize an LNA as the first block in the front end to amplify and filter the signal with a low noise addition as shown in Figure 3-8. For example, in the designs presented in [9, 13, 25, 26] an LNA is inserted at the front of the chain to achieve higher sensitivity at the cost of burning more power at RF before any down-conversion. Typically, such front-end can achieve a sensitivity better than $-80\ dBm$, however, the LNA alone burns tens of microwatts which a lot of IoT applications cannot afford.

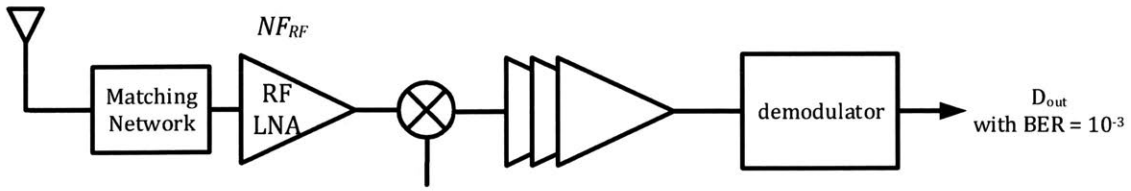


Figure 3-8: LNA-first architecture

3.2.3 Mixer-first front-end

A passive mixer as the first block in the chain comes as a very appealing front-end for an ultra-low power receiver which is depicted in Figure 3-9. It has the advantage of consuming almost no power while directly down-converting the input RF signal to IF for amplification and filtering at a much lower rate, and hence, power consumption. However, several implications arise from having the mixer switches as the very first block right after the matching network, some of these issues are presented in [29] and analyzed for performance comparison with conventional receivers.

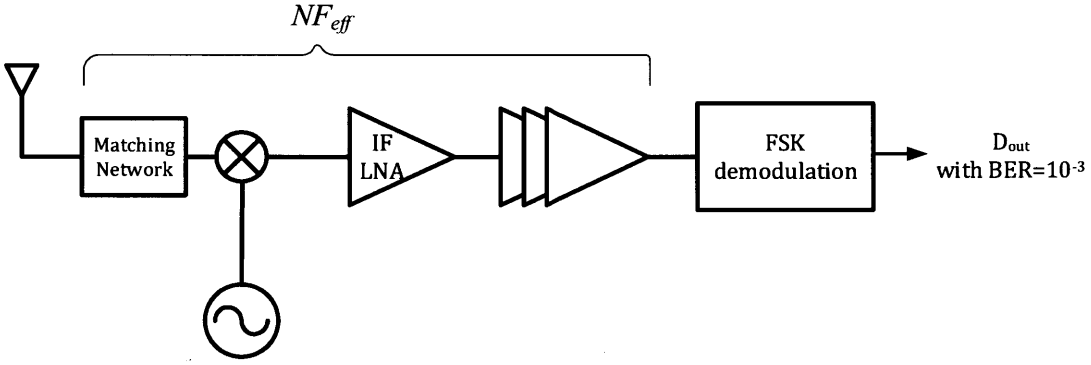


Figure 3-9: Mixer-first architecture

The first issue is the input impedance of the receiver and the matching requirements with the antenna. As derived in [29], the passive mixer is sort of transparent and its input impedance strongly depends on the baseband impedance presented to it. In addition, the reradiation back to the antenna through the mixer switches results on some dependence on the impedance at the RF port of the mixer. Thus, the matching network of mixer-first architectures must be designed carefully to account for both the load and source impedances of the mixer. The second implication is the mixer's noise figure, its bounds, and its effect on the overall system performance. Such architecture can be used in both high performance receivers as in [30] as well as low power nodes as in [31].

For example, by analyzing the system in Figure 3-9 for an FSK receiver with a required BER of 10^{-3} and assuming that the mixer-first front-end can achieve an effective noise figure of about $NF_{eff} = 13\ dB$, the required BW is derived then according to the following equations given that the required signal to noise ratio is $SNR_{req} = 7.5\ dB$:

$$P_{sens} = -174\ dBm/Hz + 10\ log(BW) + NF_{eff} + SNR_{req} \quad (3.3)$$

$$-90 = -174 + 10\ log(BW) + 13 + 7.5 \quad (3.4)$$

$$\therefore BW \simeq 2MHz \quad (3.5)$$

where the thermal noise floor is set to $-174\ dBm/Hz$ and the sensitivity (P_{sens}) is set to $-90\ dBm$. In conclusion, a small bandwidth is required to achieve high sensitivity and account for the inherently lower NF of the mixer-first architecture.

3.3 Proposed architecture

In conclusion, several receiver architectures are available in the literature, each is targeting a certain application or performance enhancement. By exploring the available options, an architecture for the BLE wake-up receiver is proposed in Figure 3-10 where the following design choices are made:

- **Uncertain-IF architecture:** a low-power free running oscillator is utilized to generate the local oscillator (LO) for the whole receiver chain.
- **Mixer-first front-end:** a passive mixer is chosen as the first block of the chain for its ultra low power, possibility of matching, and down-conversion for lower rate processing.
- **Programmable N-path IF filter:** along the receiver chain programmable N-path filters [32] are used for IF filtering so that they can be tuned according

to any variations in the free running oscillator.

- **Programmable FSK demodulator:** the FSK demodulator needs to be programmable as well to track the oscillator and the IF bandwidth of the system.
- **Security Engine:** an off-chip engine for generating a one-time wake-up pattern is implemented on an FPGA for providing the wake-up sequence for the IoT node.

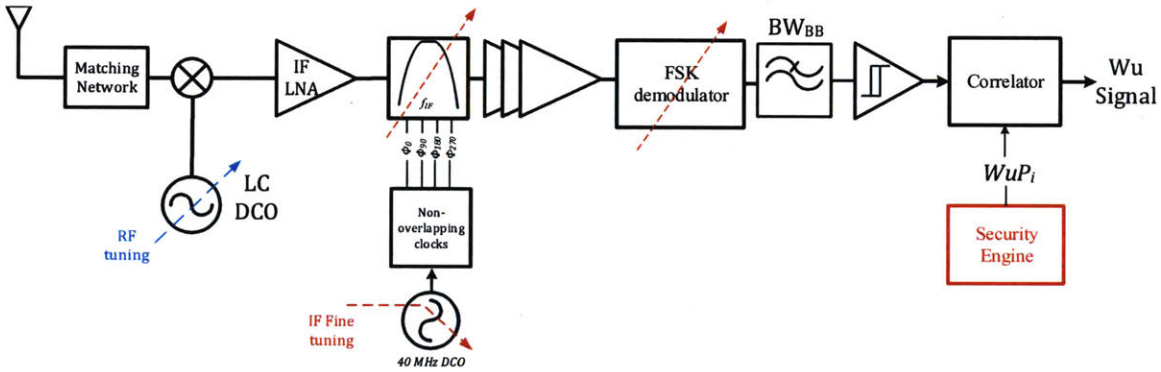


Figure 3-10: Proposed system block diagram for the wake-up receiver

Chapter 4

Circuit-level implementation

Moving one step further in the system developed in the last chapter, this chapter illustrates the circuit-level implementations of the individual building blocks of the wake-up receiver.

4.1 Wake-up receiver system

Building up on the proposed system in Chapter 3, the proposed block diagram of the wake-up receiver system is illustrated in Figure 4-1. As shown, the wake-up receiver makes use of an off-chip security engine to generate a new wake-up sequence every wake-up event which will be described later. In the following sections, this block diagram is dissected into smaller building blocks where the circuit choices, trade-offs and block-level performance are presented throughout the whole receiver chain. The flow starts by the passive mixer front end and then moves to the free-running oscillator driving it. Next, it switches to the IF band where amplification, filtering and demodulation occurs. Finally, it reaches the baseband processing with the final correlation for the wake-up detection.

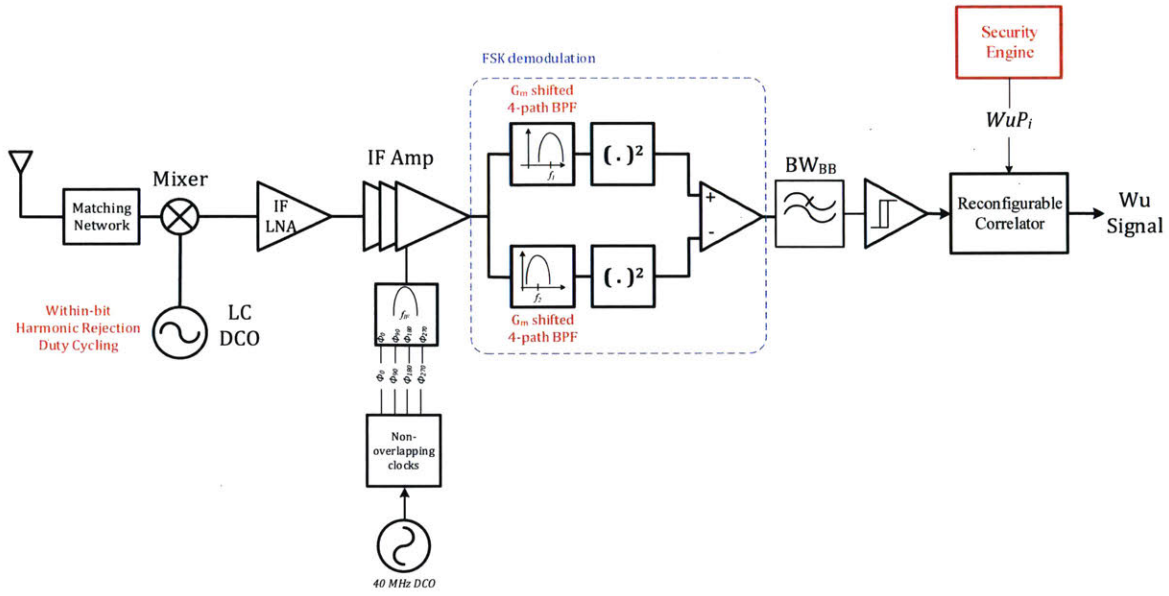


Figure 4-1: Proposed system block diagram for the wake-up receiver

4.2 Mixer-first front end

As mentioned in the previous chapter, implementing a passive mixer as the first block in the receiver chain requires the design of the mixer in conjunction with the matching network as well as the next IF LNA block due to the mixer's transparency.

The wake-up receiver front-end is shown in Figure 4-2 where an L-section matching network is used both to match the antenna with the input impedance of the chain and also to provide a passive gain to improve the overall sensitivity. In particular, a matching network which transforms an antenna impedance of $Z_0 = 50\ \Omega$ into an input impedance of Z_{in} provides at the same time a passive gain of:

$$A_{passive} = \sqrt{\frac{Z_{in}}{Z_0}} \tag{4.1}$$

Hence, a bigger input impedance is preferable for a higher passive gain.

From [29], the input impedance of the passive 2-phase mixer is given by:

$$Z_{in} = R_{sw} + \gamma Z_B \parallel R_{sh} \tag{4.2}$$

where R_{sw} is the switch resistance, $Z_B = \frac{1}{j\omega C} \parallel Z_{IF}$ is the input impedance at the IF port, γ is an impedance transform term accounting for the linear time varying nature of the switches, and R_{sh} is a virtual shunt impedance accounting for the dependence on the antenna impedance. This means that there is a trade-off here between the switch noise and the passive gain as the noise requires R_{sw} to be low while the passive gain is in favor of having a bigger switch resistance. Thus, a compromise has to be made to size the transistor for sufficient gain and adequate noise figure.

Therefore, equation (4.2) can be used to choose the matching network components, the switch resistance and adjust the input impedance of the IF LNA accordingly to get the correct gain and matching requirements.

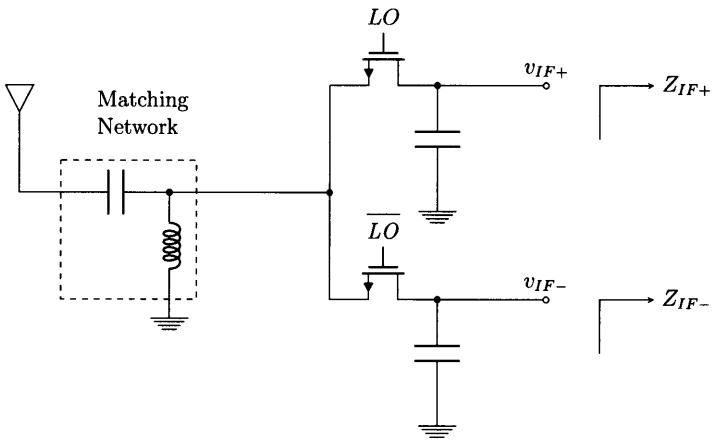


Figure 4-2: Passive mixer circuit

A 2 pF capacitor is used as the mixer load to limit out of band interference, while a matching network of values $L = 14\ nH$ and $C = 297\ fF$ are chosen to achieve a matching better than $-11\ dB$ as shown in Figure 4-3 while providing a passive gain of almost 11 dB around the signal band as shown in Figure 4-4.

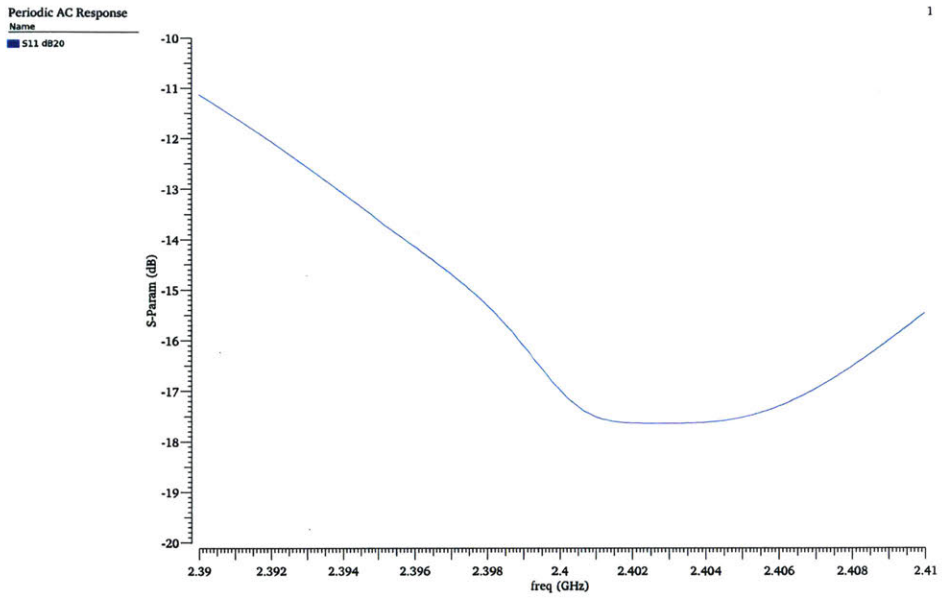


Figure 4-3: S11 parameter of the receiver showing the matching BW

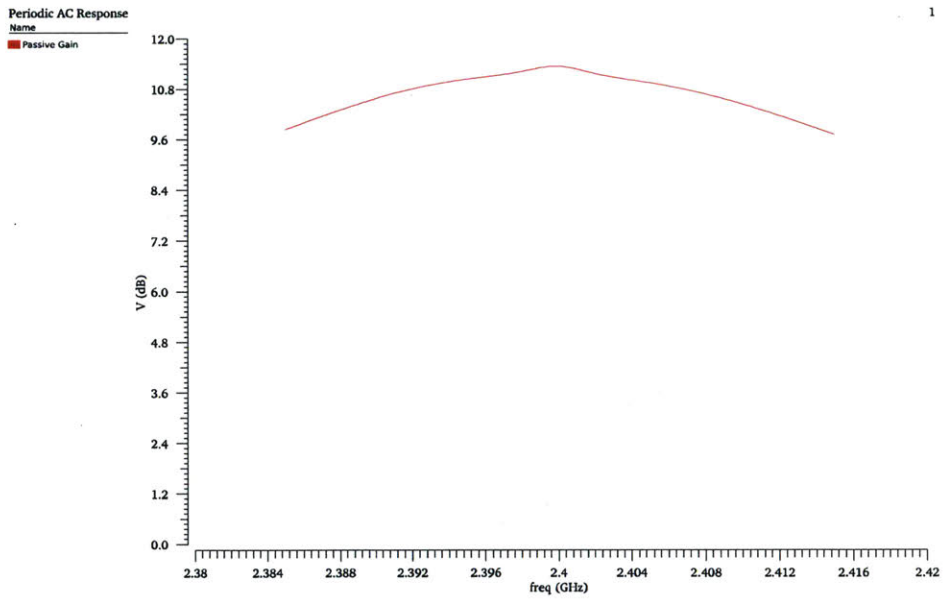


Figure 4-4: Passive gain of the matching network preceding the mixer circuit

4.3 Free-running oscillator

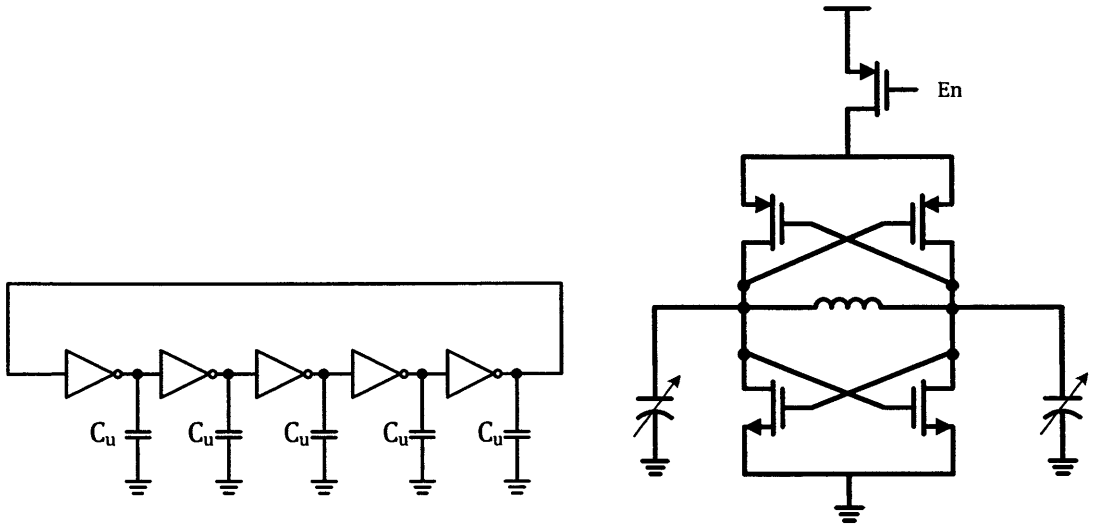
A free-running oscillator serves as the best candidate for ultra low power operation where all the blocks of a complete PLL are dropped to ensure huge energy savings. This section presents oscillator architectures and develops a new duty cycling method for further savings.

4.3.1 LC Oscillator vs Ring Oscillator

The two main candidates for the digitally controlled oscillator (DCO) are the LC oscillator and the ring oscillator. Each architecture has its own merits but suffers from particular drawbacks. For instance, the ring oscillator design is a simple loop of an odd number of cascaded inverters as shown in Figure 4-5a. The frequency of oscillation can then be controlled by varying the unit capacitance at each node (C_u), utilizing the current starving technique, or just changing the supply voltage of the inverters. With an almost fully digital design, such architecture takes advantage of all the digital circuit benefits gained from technology scaling. The power consumption is merely the dynamic power due to switching, short circuit current drained during transitions, and the leakage power consumed during the off time. Thus, the voltage and technology scaling makes the ring oscillator a highly energy efficient architecture. Unfortunately, this efficiency comes at the expense of frequency accuracy. As derived in [33], the jitter of the ring oscillator is bigger than its LC counterpart. Hence, an uncertain IF architecture which utilizes a ring oscillator suffers from a huge uncertainty in its IF BW that can reach up to almost 100 MHz as in [2,9].

On the other hand, the LC oscillator provides a much stable frequency governed by the value of its inductance and load capacitance ($\omega_0 = \frac{1}{\sqrt{LC}}$). A generic LC oscillator circuit is shown in Figure 4-5b where cross-coupled nmos and pmos pairs are used to provide a negative resistance effect which nullifies the series resistance of the inductor and ensures that the oscillation criterion is met. Contrary to the ring oscillator, the voltage scaling pushes the LC oscillator to its limits instead of benefiting it. A squeezed voltage supply produces a limited voltage swing while more current might be needed to get the required transistors transconductance at the same current level.

Figure 4-6 illustrates the phase noise performance of the LC oscillator showing a value of $-110.2\ dBc/Hz$ at an offset of $\Delta f = 1\ MHz$. In addition, the work in [3] shows that the instantaneous measured frequency of a free-running LC oscillator varies



(a) Five-stage Ring Oscillator circuit (b) Cross-coupled LC Oscillator circuit

Figure 4-5: Oscillator architectures

slowly in a bound of about 70 kHz during hours of measurement. Therefore, an uncertain IF architecture with an LC oscillator as its free running oscillator can be designed for a high sensitivity operation with a small uncertain bandwidth and hence, lower noise bandwidth.

In order to further reduce the constant DC power consumption of the oscillator, an enable pmos switch is added between the oscillator and the supply in order to turn off the oscillator whenever not needed and reduce the average power. In addition, a tail current source is added to set a value for the DC current in the cross-coupled pairs and control the total power being consumed.

4.3.2 LO Buffers

The low voltage LC oscillator can't drive the mixer switches directly, it requires a buffering circuit which is tapered to be able to drive the gate capacitance of the switches. Such circuit is depicted in Figure 4-7 where a self-biased inverted is used as the first block to amplify the LO signal regardless of its DC level. Then, it is followed by a cascade of inverters tapered by a ratio of 2 till it reaches the load capacitance.

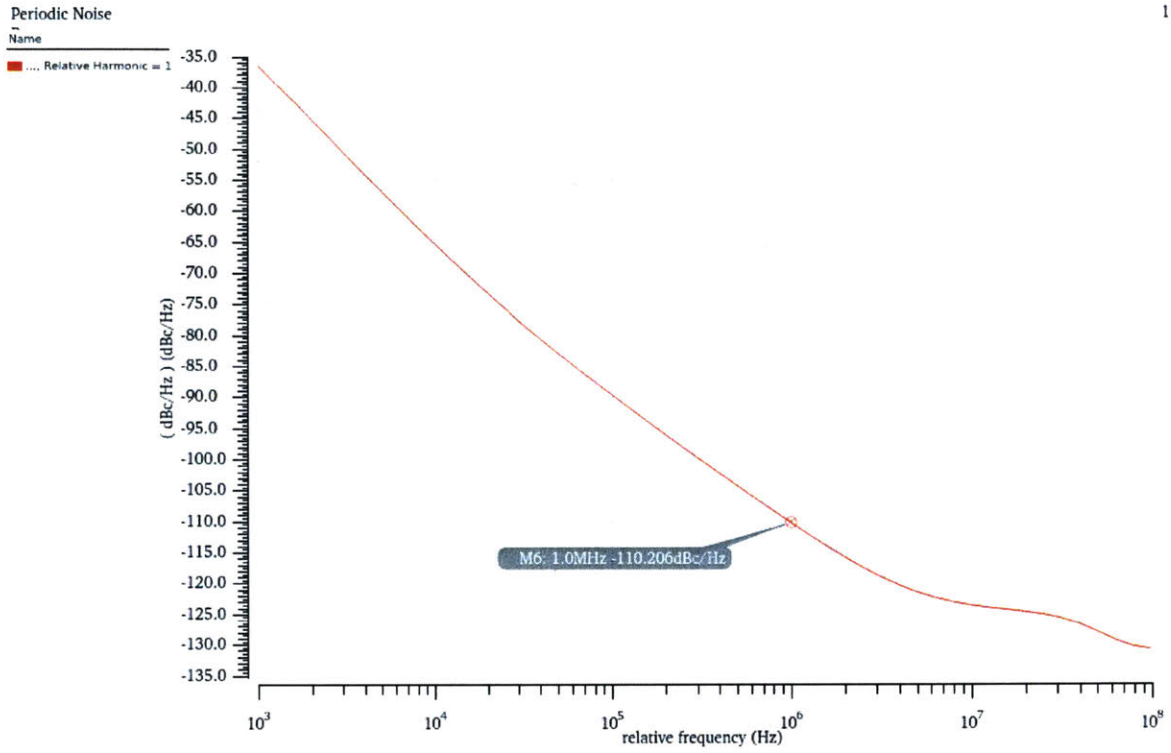


Figure 4-6: LC Osc Phase Noise performance

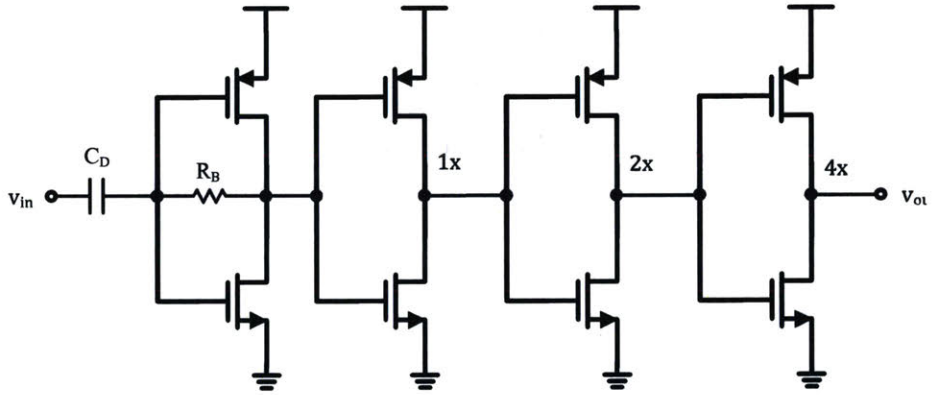


Figure 4-7: LO buffer circuit

4.4 IF LNA

The IF LNA is the second block in the chain directly after the passive mixer and its closed loop input impedance has a direct impact on the receiver's impedance and the design of the matching network. In consequence, the biasing resistor (R_{IF})

shown in Figure 4-8 is also taken into consideration in choosing the matching network components. A current reuse architecture is utilized to take full advantage of the transconductance of both the NMOS and PMOS input transistors (g_{mN} and g_{mP} respectively) to get a higher effective transconductance ($g_{m,eff}$) at the same current.

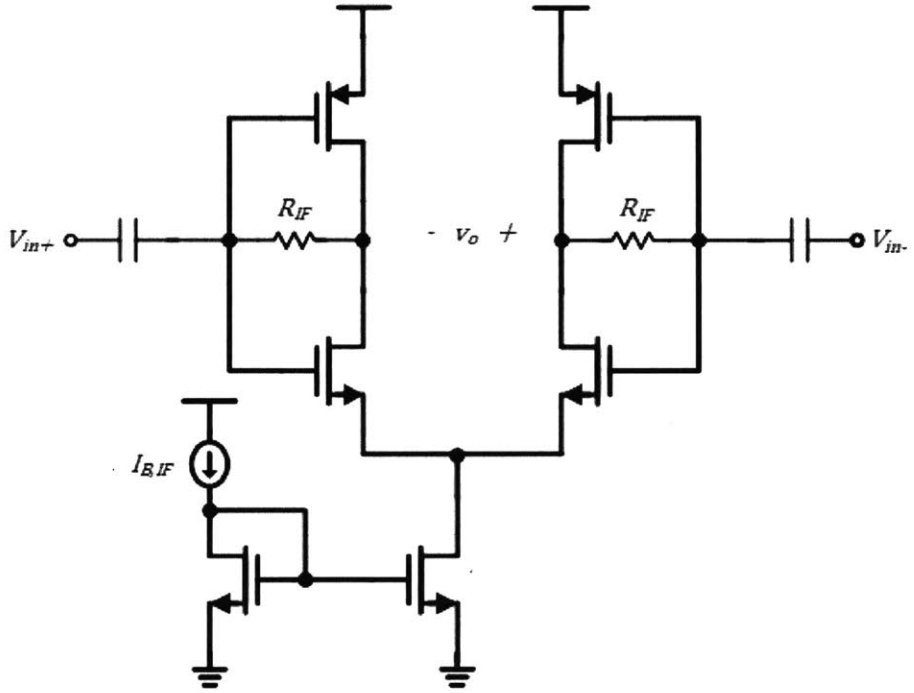


Figure 4-8: IF LNA circuit schematic

4.5 IF bandpass filter

As the signal undergoes down-conversion to IF and gets amplified by the IF LNA, it needs to be filtered to reject any out of band interferers and to reduce the overall noise BW in order to achieve the required sensitivity. Hence, the block directly following the LNA has to be a bandpass filter (BPF) that is programmable enough to track the free-running oscillator variations while narrow enough to limit the noise and interference over the whole chain.

4.5.1 N-path BPF

A programmable BPF can be implemented using an N-path filter which is basically a switched capacitor filter whose center frequency depends on the switching clock frequency. A 4-phase BPF is shown in Figure 4-9 which operates nominally at the IF of 10 MHz and the clock is reconfigured according to any variations in the LO frequency. The operation of such N-path filter can be analyzed using the model in [32] where the system behaves as an equivalent RLC network with a band pass filter response. The filter operation can be divided into two steps: in the first one, the signal is down-converted by the 4-path switches and then low-pass filtered by the baseband capacitors (C_{BB}); in the second step, the filtered signal gets up-converted through the same switches to the output node (v_{out}).

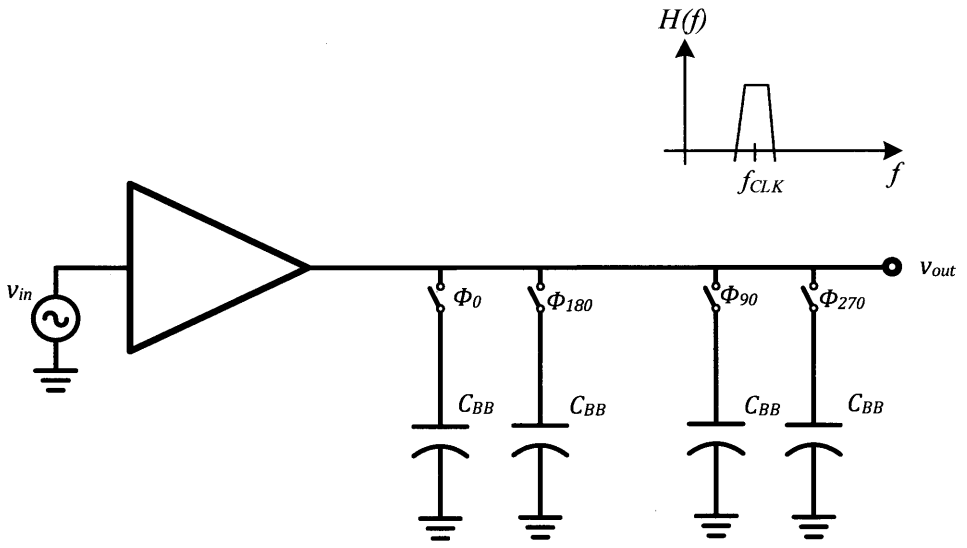


Figure 4-9: 4-path IF bandpass filter

The periodic steady state frequency response simulation of the IF band-pass filter is shown in Figure 4-10 where the filter is centered around the clock frequency which can be adjusted according to the system's variations.

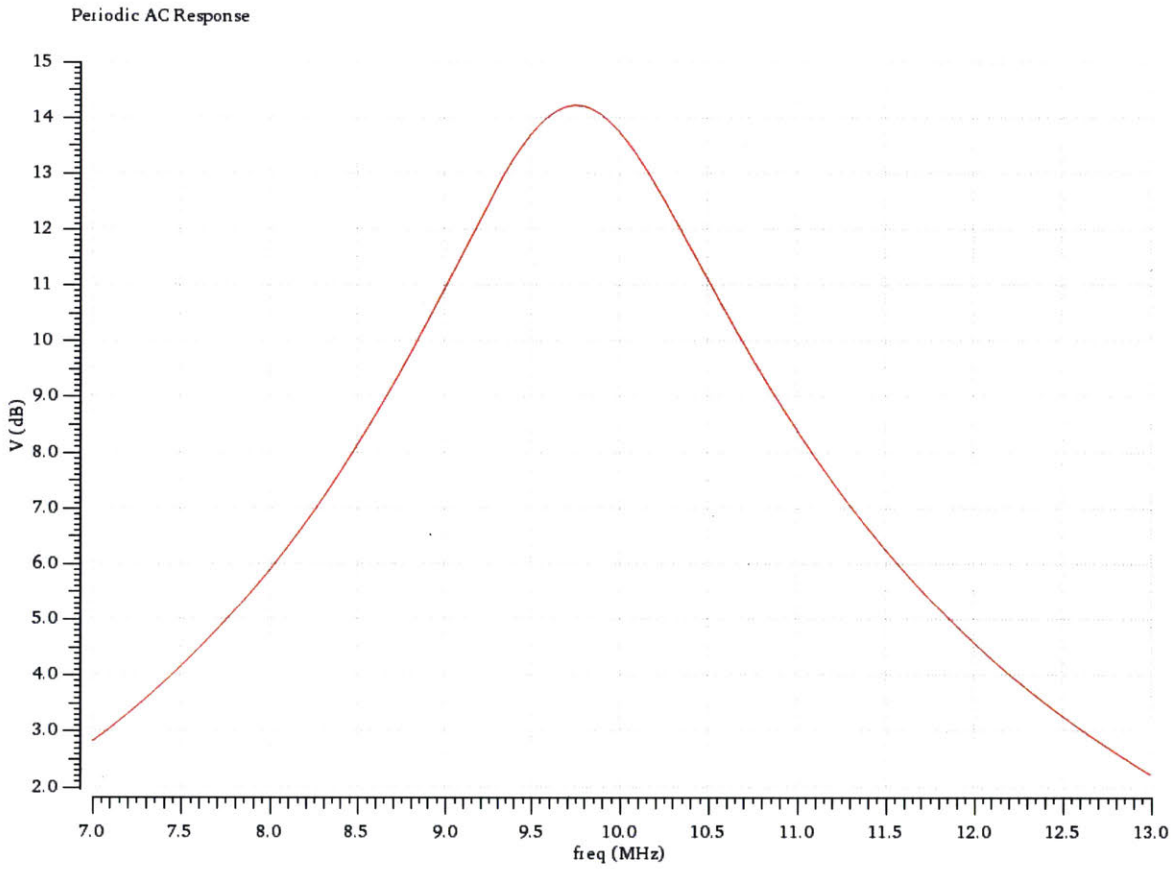


Figure 4-10: Frequency response of the 4-path IF bandpass filter

4.5.2 Clock generation

Four non-overlapping clocks need to be generated for all the IF filtering as well as the FSK demodulation circuitry. As the IF is designed to be at 10 MHz, then a 40 MHz clock is generated using a ring digitally controlled oscillator and the circuit schematic for such oscillator is shown in Figure 4-11 where the control bits are initially adjusted for a nominal frequency of 40 MHz. Then, the circuit in Figure 4-12 is used to produce four 90° out-of-phase signals at 10 MHz. The DCO is implemented as a ring of odd number of current starving inverters with an 8-bit control to have enough programmability for the IF uncertainty as well as the ring oscillator variation itself.

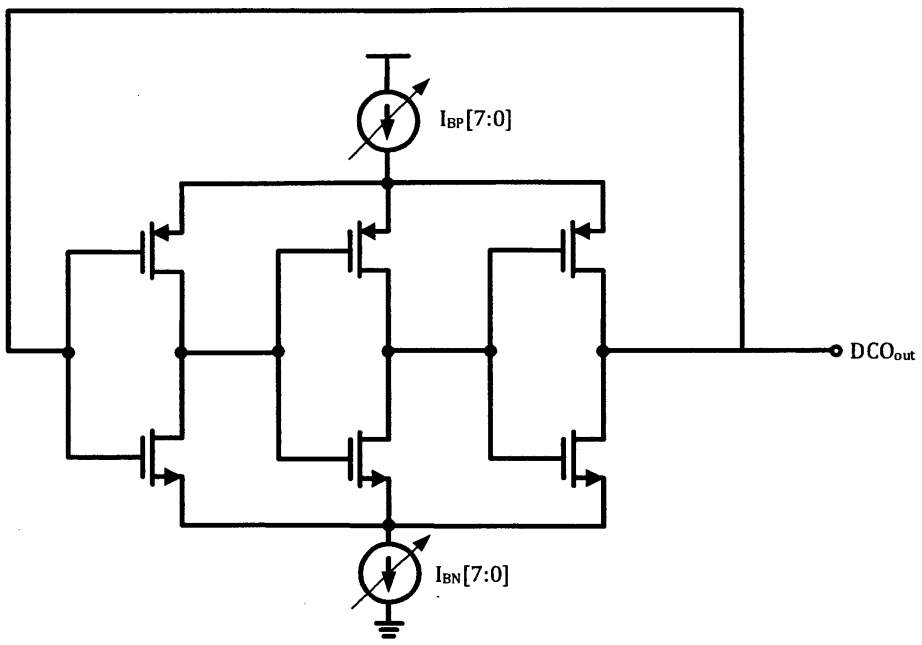


Figure 4-11: IF digitally controlled ring oscillator

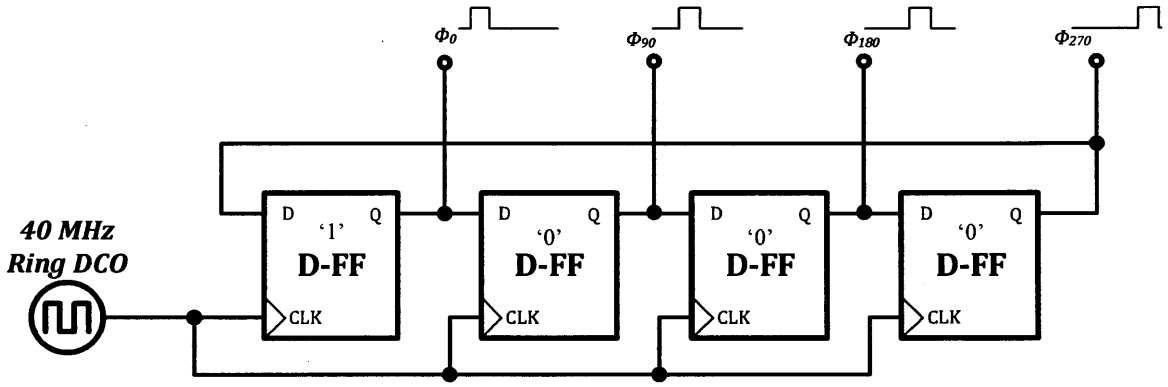


Figure 4-12: 4-phase clock generation

4.6 IF variable gain amplification

A variable gain amplifier (VGA) is needed in the receiver chain in order to control the total chain gain and prevent saturation at different input signal levels. An amplifier with selective source degeneration is designed as shown in Figure 4-13 where the switches select the required degeneration resistance value and a resistive common

mode feedback composed of R_{CMFB} resistors is used to set the output bias point [3]. The gain then is given by:

$$A_{VGA} = \frac{g_{m,nmos}R_{out}}{1 + g_{m,nmos}R_{degen}} \tag{4.3}$$

$$R_{out} = r_{o,n} \parallel r_{o,p} \parallel R_{CMFB} \tag{4.4}$$

$$R_{degen} = 0, R_1, or R_2 \tag{4.5}$$

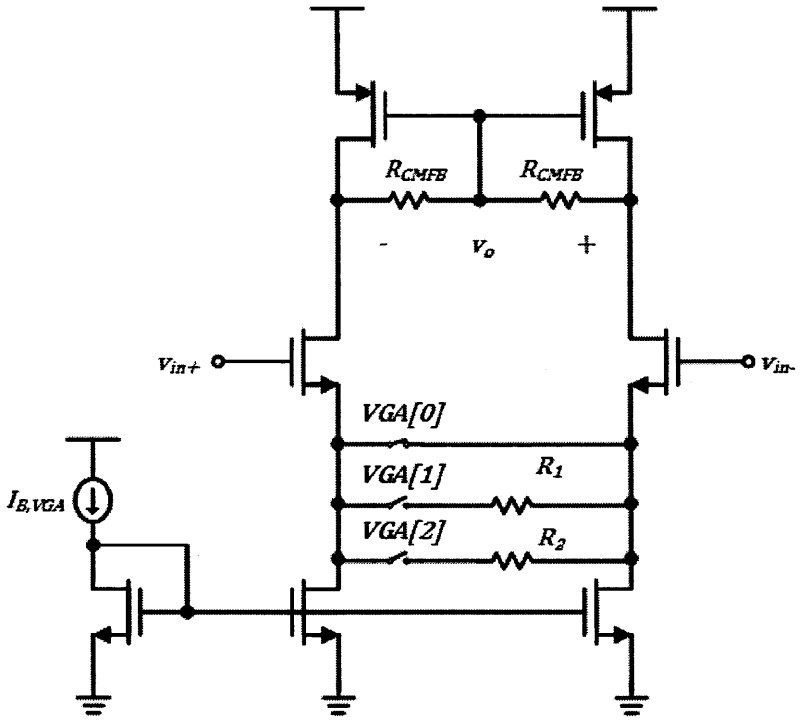


Figure 4-13: IF VGA circuit schematic

Hence, the VGA control bits ($VGA[2:0]$) can be controlled to adjust the chain overall gain according to the the received signal level.

The frequency response of the IF VGA at different configurations is shown in Figure 4-14 where the gain can vary from almost 20 dB down to 4 dB at the highest degeneration.

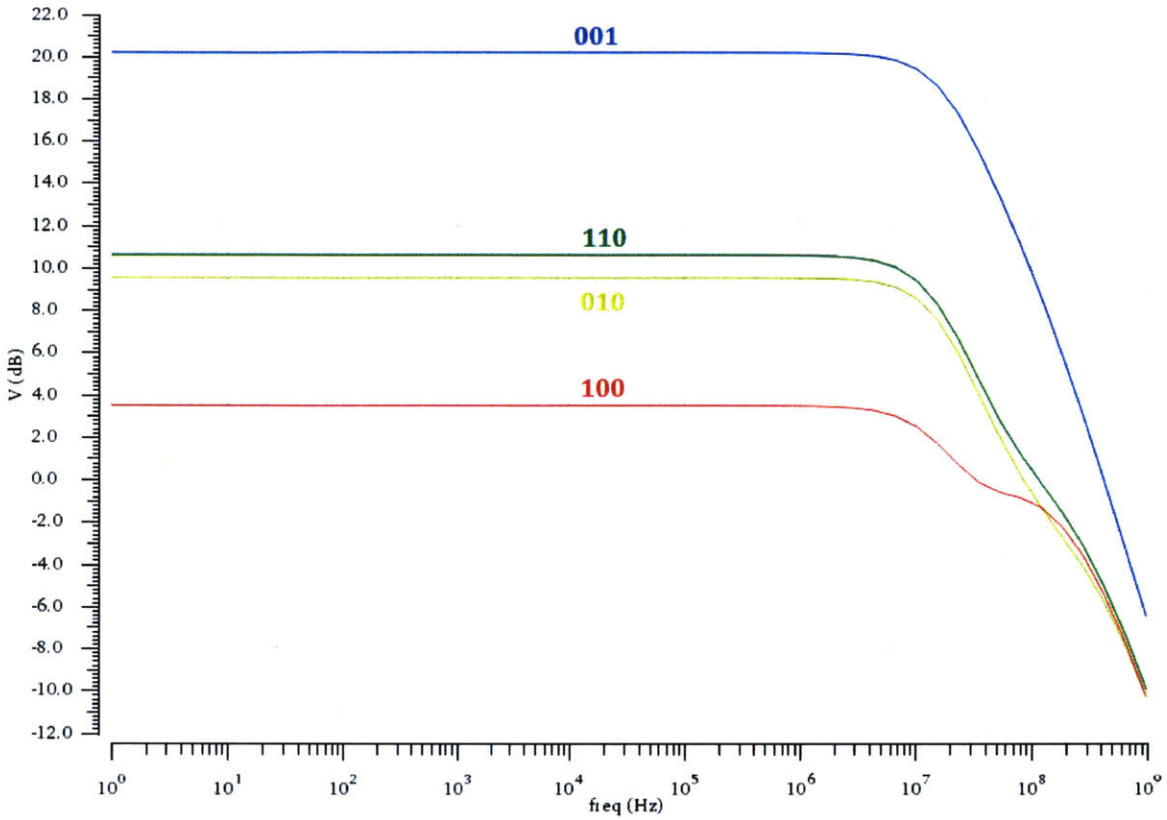


Figure 4-14: Frequency response of VGA at different configurations

4.7 FSK demodulator

Following all signal amplification and channel selection filters, the GFSK modulated BLE packets must then be demodulated in order to extract the actual transmitted bits from the base station to be able to detect any wake-up packets.

4.7.1 Bit repetition for low datarate

Due to the low rate nature of the IoT applications and the fact that the BLE packets are transmitted at a 1 $Mbps$ with a GFSK modulation of a 500 kHz frequency deviation, a new scheme has to be developed such that the receiver can still be BLE-compliant while the data rate is adjusted according to the application's needs.

In this thesis, the data rate is designed to be almost 333 $kbps$ with a bit duration of 3 μs and can be adjusted to be 6 μs. This is achieved through bit repetition by

sending 3 bits for 1 bit and de-whitening of the raw data in order to counteract the whitener which already exists at the transmitter side. Then, by using such technique the wake-up receiver can detect the wake-up sequence as well as some control bits sent on the same packet. Through correlation with the predetermined wake-up sequence, a synchronization is achieved and used to decode the input bits.

4.7.2 FSK N-path BPFs

As the frequency deviation is fixed to 500 kHz while the datarate is adjusted to be around 333 *kbps* by using bit repetition, then FSK demodulation can utilize simply two narrow band BPFs with a 500 kHz difference between their center frequencies followed by an energy detection and comparison circuit to detect which frequency is being transmitted with the '1' bit being the higher frequecny as stated by the BLE standard [34]. The FSK demodulator block diagram is shown in Figure 4-15 where at an IF of 10 MHz, one filter is centered around 10.25 MHz while the other is centered around 9.75 MHz.

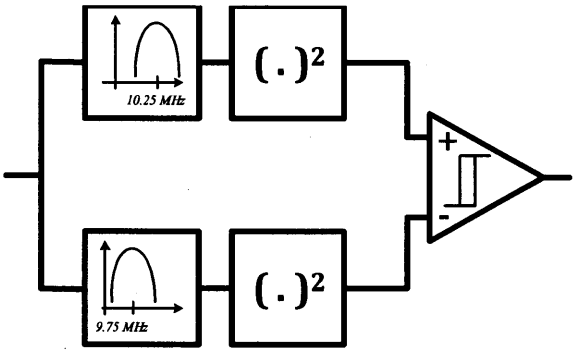


Figure 4-15: FSK demodulator circuit

Designing two BPFs is an easy task, however, having them both be programmable to track the uncertainty in the IF is not as straightforward. Exploiting N-path filters driven with a programmable DCO will provide a solution but the overhead in power and area of having two different oscillators might outweigh its programmable

advantage.

A new circuit needs to be developed to design two narrow band BPFs with programmable center frequencies without much overhead. By using the programmable N-path filters and the technique described in [35] which utilizes transconductance cells (Gm-cells) to shift the center frequency of the N-path filter around the clock frequency of the switches. Such technique is shown in Figure 4-16 where two differential Gm cells are used to control the center frequency shift away from the clock frequency.

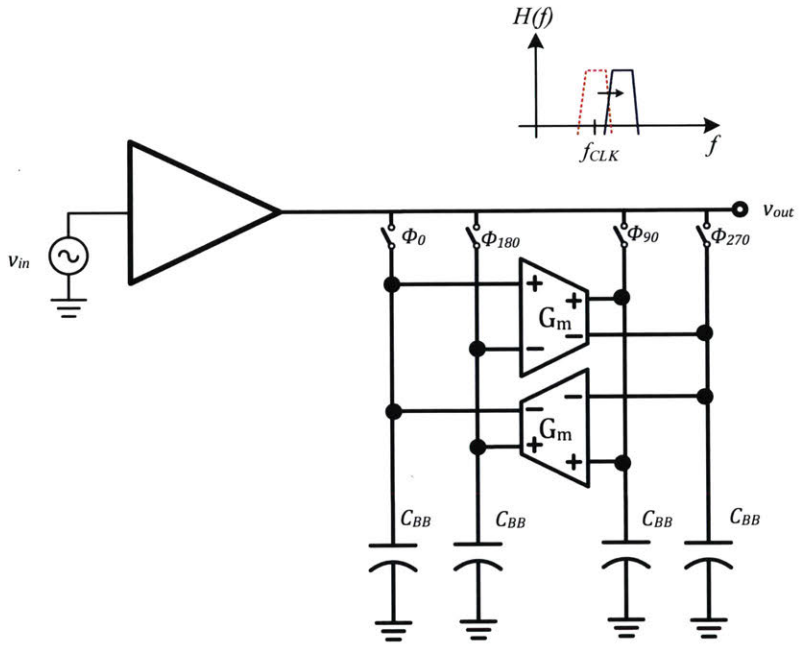


Figure 4-16: G_m-shifted band-pass filter

By adding the Gm-cells, the input impedance of the switched capacitor load changes from capacitive to a complex impedance mimicking a frequency shift in the BPF center frequency. For instance, a conventional switched capacitor filter with a load capacitor of C_{BB} forms a low pass filter with the switch resistance and then the mixing effect upconverts this filter response around the clock frequency f_{CLK}.

By adding the Gm-cells, then the impedance around the clock frequency f_{CLK}

becomes

$$Y_{Gm}(s) = \frac{1}{Z_{Gm}(s)} = sC_{BB} - jG_m = C_{BB}(s - j\omega_{BB}) \quad (4.6)$$

$$where \quad \omega_{BB} = \frac{G_m}{C_{BB}} \quad (4.7)$$

which means that a positive frequency shift of ω_{BB} can be achieved by having a positive G_m value while a negative frequency shift is attainable through an opposite-sign differential G_m structure. Therefore, two narrow band BPFs with the required frequency deviation can be designed to detect either a transmitted '1' or '0' bits. The center frequency programmability is shown in Figure 4-17 for positive and negative transconductance values.

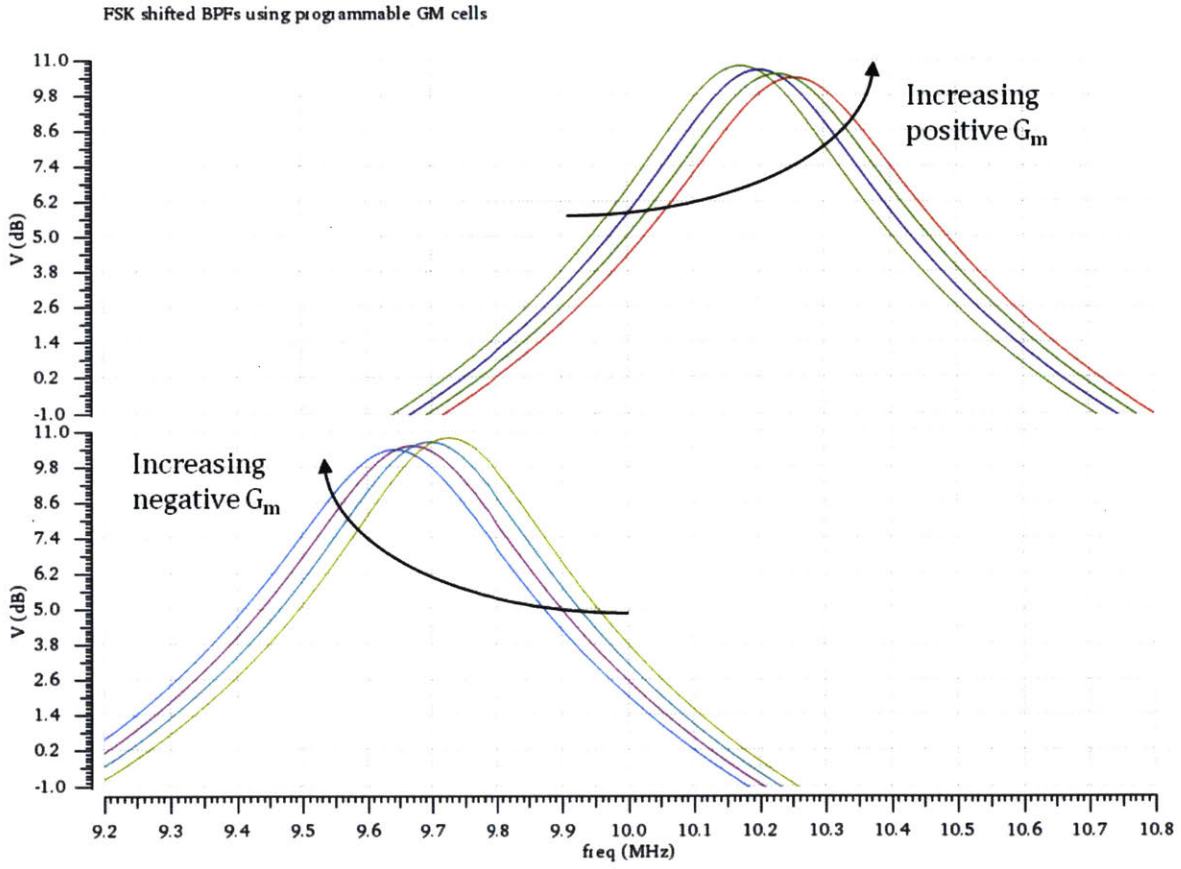


Figure 4-17: Frequency response simulation of G_m-shifted band-pass filter at different Gm values

The G_m cells employ a differential pair with programmable source degeneration such that their values can be adjusted accordingly to get the BPFs centered at 9.75 MHz and 10.25 MHz as shown in Figure 4-18.

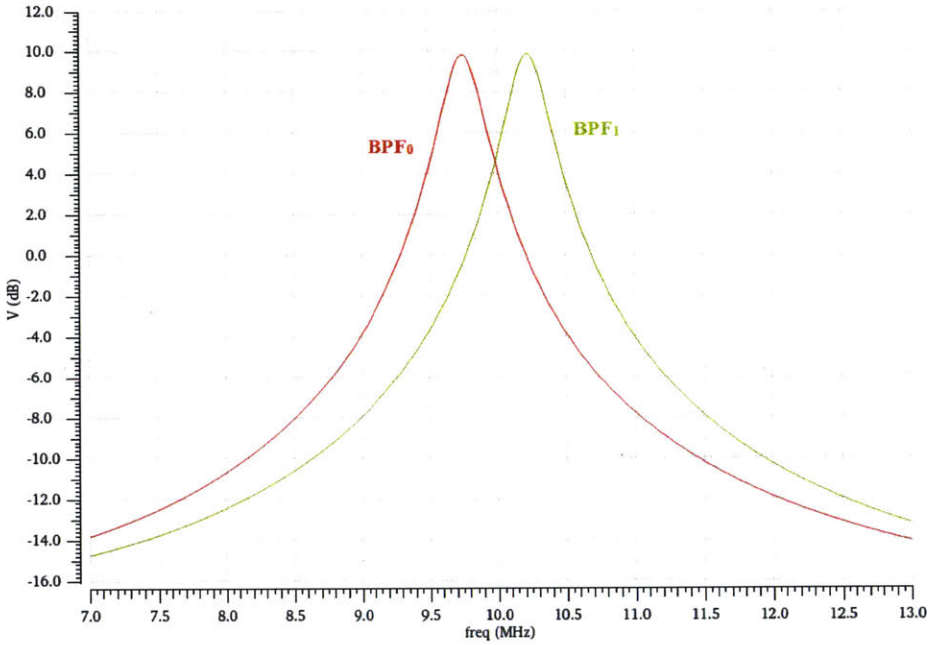


Figure 4-18: Frequency response simulation of the BPFs adjusted for the GFSK detection

4.8 Reconfigurable Correlator

A 32-bit correlator is designed as shown in Figure 4-19 where an input reconfigurable wake-up pattern is correlated with the input bits to determine whether the correlation between the input bits and the pattern is below a pre-determined threshold or not. Hence, if the correlation is above the threshold, a wake-up signal is generated to the sleeping node. Otherwise, then the wake-up packet is destined for another IoT node.

A bank of three correlators is used to account for the phase shift between the input bits and the pre-determined wake-up pattern.

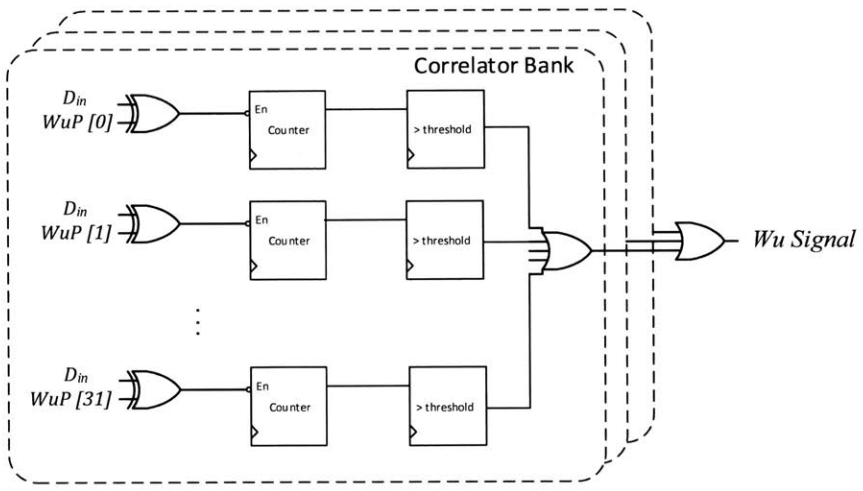


Figure 4-19: Correlator circuit showing the wake-up pattern correlator banks

4.9 System results

In this section, the simulations for the whole receiver chain is presented showing the transient operation, the noise performance and power breakdown then evolves to develop a new duty cycling scheme to tackle the main power consuming blocks.

4.9.1 Noise simulation

The in-band noise figure for the whole chain is simulated to make sure that the overall noise performance satisfies the $-90\ dBm$ sensitivity defined by the system requirements according to equation (3.5). For this level of sensitivity and a $BW = 2\ MHz$ the whole chain effective noise figure should be less than 13 dB. The noise simulation of the whole chain from the antenna all the way to the FSK demodulator is depicted in Figure 4-20 where the NF for the whole bandwidth is almost 9.5 dB.

4.9.2 Transient simulation

A transient simulation for the receiver chain is also conducted to check the system functionality. An input random pattern, shown in the first trace of Figure 4-21, is

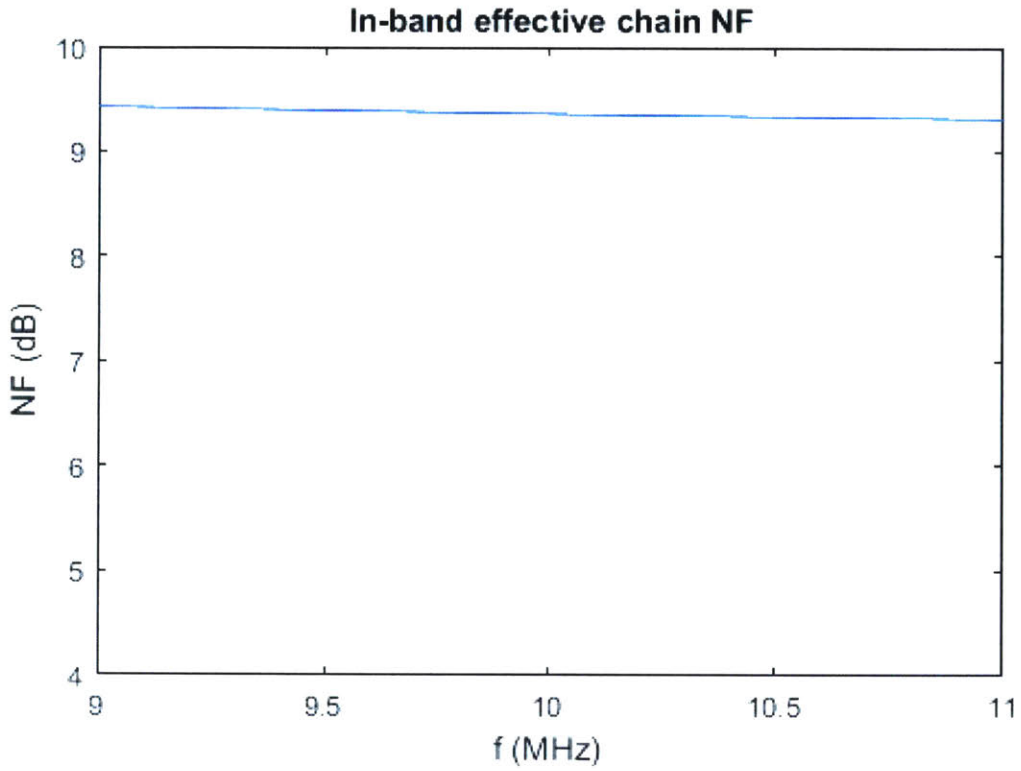


Figure 4-20: NF simulation of the whole system till the FSK demodulator

modulated at 2.41 GHz and then used to excite the system at a power of -90 dBm. The signal then gets amplified and filtered till it reaches the demodulator BPFs where one is high at the '1' frequency while the other is low and vice versa as shown in the second subwindow. Then the envelope detector detects the energy in each band with the amplified difference shown in the third subwindow. Finally, a Schmitt trigger inverter produces the bit which is then sampled by a flip-flop with a $3\times$ oversampling.

4.9.3 Active Power breakdown

The whole receiver chain consumes an overall active power of about 180 μW and the power breakdown of the individual components is shown in Figure 4-22. This power level is still much higher than the required sub-μW consumption. By analyzing the percentage consumed by each block, it is quite obvious that the LC oscillator and its

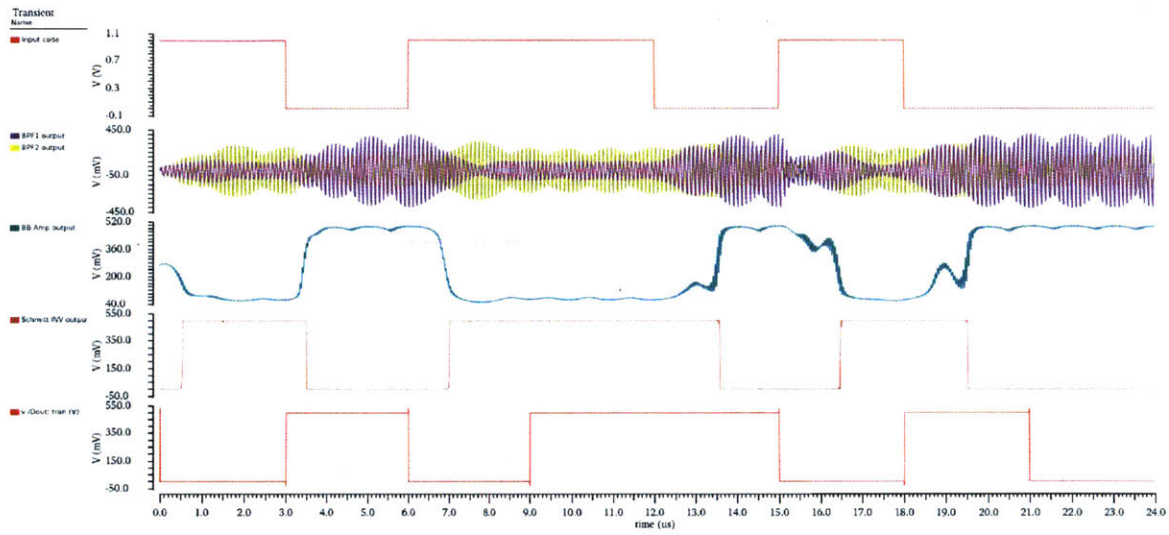


Figure 4-21: Transient simulation of the whole system

auxiliary circuits of buffers consume together 80% of the total active power. Therefore, in order to break down such power limits, the consumption of the oscillator must be tackled and further reduced as much as possible which will directly impact the total active power.

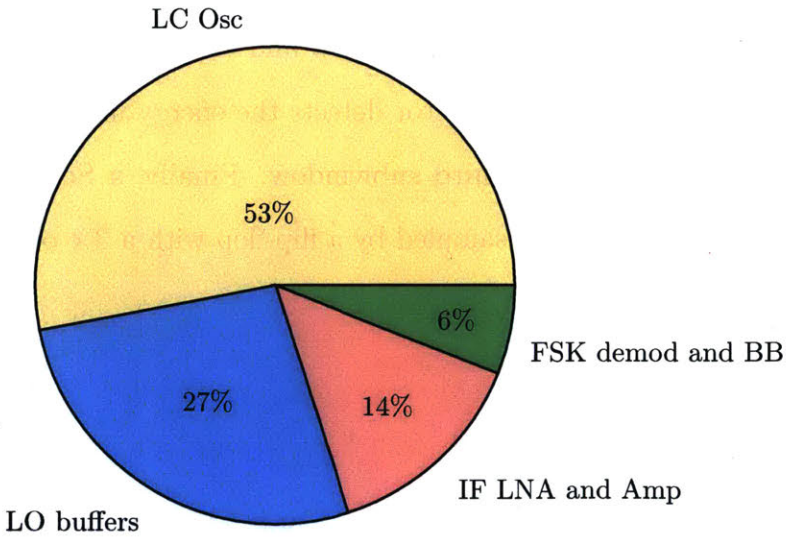


Figure 4-22: Breakdown of the receiver's active power consumption

4.9.4 Within-bit Duty cycling

Further reduction of average power consumption can take advantage of the fact that the IoT transmission usually operates at a quite low data rate. This means that one symbol can take up to few microseconds or even tens of microseconds. Hence, a new within-bit duty cycling scheme is proposed which turns off the oscillator, the main consumer of power, during the long bit duration and back on just to ensure correct bit detection while reducing the average power.

Within-bit oscillator duty-cycling can be implemented using a PMOS switch to act as an enable to the whole oscillator and its buffers as in Figure 4-5b. Such implementation can be used for a 50% duty cycling scheme to save almost half the power the consumption of the receiver, as shown in Figure 4-23, given that the oscillator and its buffers consume almost 80% of the total receiver power. Unfortunately, this duty-cycling scheme produces a lot of harmonics in the oscillator's waveform which in turn causes the mixing of noise and interferers at these frequencies to fold back into the signal band degrading the overall receiver's sensitivity. This can be directly inferred from the Fourier series of the waveform of the duty-cycling signal given by:

$$f_{DutyCycling}(t) = \frac{1}{2} + \frac{1}{\pi}\sin(\omega t) + \frac{1}{3\pi}\sin(3\omega t) + \frac{1}{5\pi}\sin(5\omega t) + \cdots \tag{4.8}$$

One technique to improve the duty cycled oscillator's spectrum is to implement a more elaborate duty cycling scheme with less power over its frequency harmonics. A harmonic rejection duty-cycling scheme is presented in Figure 4-24 where the active duration and the sign of oscillation is controlled in order to eliminate the third harmonic component leaving only a weak fifth harmonic with negligible noise and interference overhead as derived in the Fourier series of such waveform:

$$f_{harmonic}(t) = \frac{\sqrt{3}}{\pi}\sin(\omega t) + 0 - \frac{\sqrt{3}}{5\pi}\sin(5\omega t) + \cdots \tag{4.9}$$

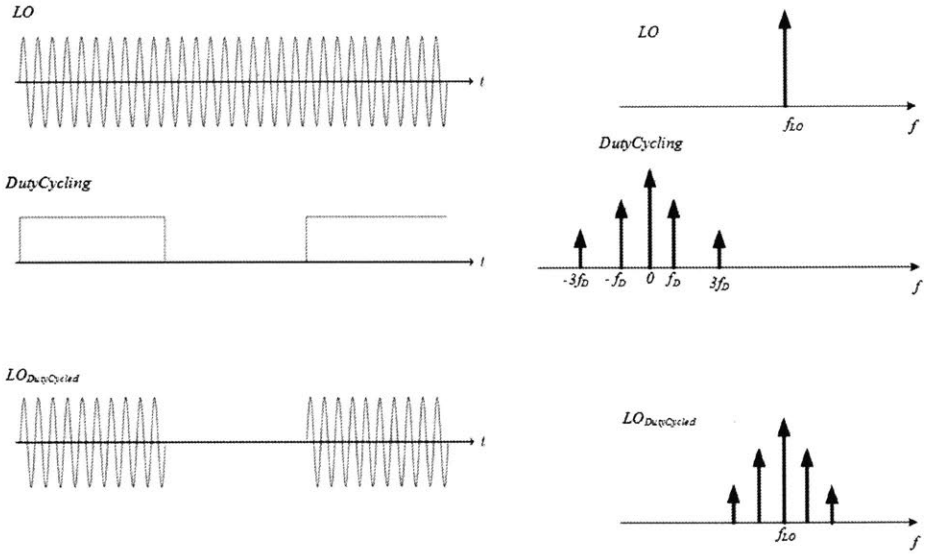


Figure 4-23: Spectrum of an LC Oscillator with 50% duty-cycling

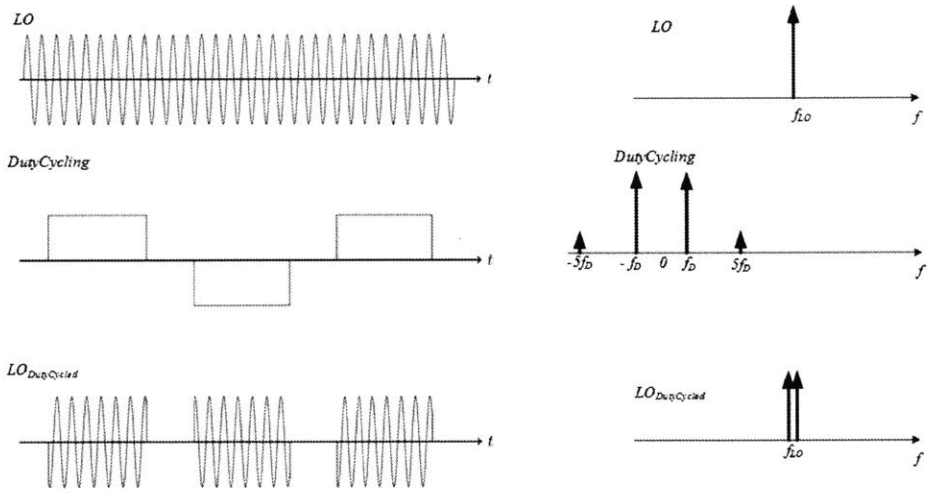


Figure 4-24: Spectrum of an LC Oscillator with harmonic-rejection duty-cycling

However, one thing here that cannot be controlled is the initial phase of oscillation. Whenever the enable switch is turned on, the initial phase depends on the circuit noise at this instant and any branch can start stronger than the other till oscillations become steady. By dividing the enable switch into a separate switch for each branch, then at turn on, the initial phase of oscillation can be selected by enabling one branch first and hence ensuring that this branch is stronger and the oscillation is biased towards this

direction of phase. Then by utilizing this scheme presented by the circuit schematic in Figure 4-25, the harmonic rejection duty cycling scheme can be implemented to reduce the power consumption without having too much harmonic components and noise folding into the band of interest.

Simulations for single enable switch startup is shown in Figure 4-26a where the phase between the different overlaid waveforms is completely random and depends on the circuit noise. On the other hand, the simulation for the the branch enabling scheme is shown in Figure 4-26b where the initial phase is controlled to make sure one branch always turns on before the other producing the same initial phase. In addition, by selecting the other branch to turn on first, then a initial phase with a 180° shift can also be produced as well. This allows for different harmonic rejection duty cycling schemes to be employed such as the one shown in Figure 4-24 or any other scheme that generates less harmonics using positive and negative shifted square waves for the duty cycling signal.

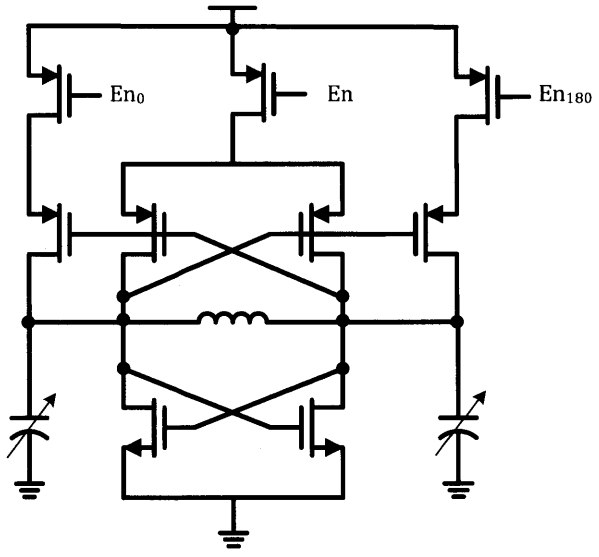
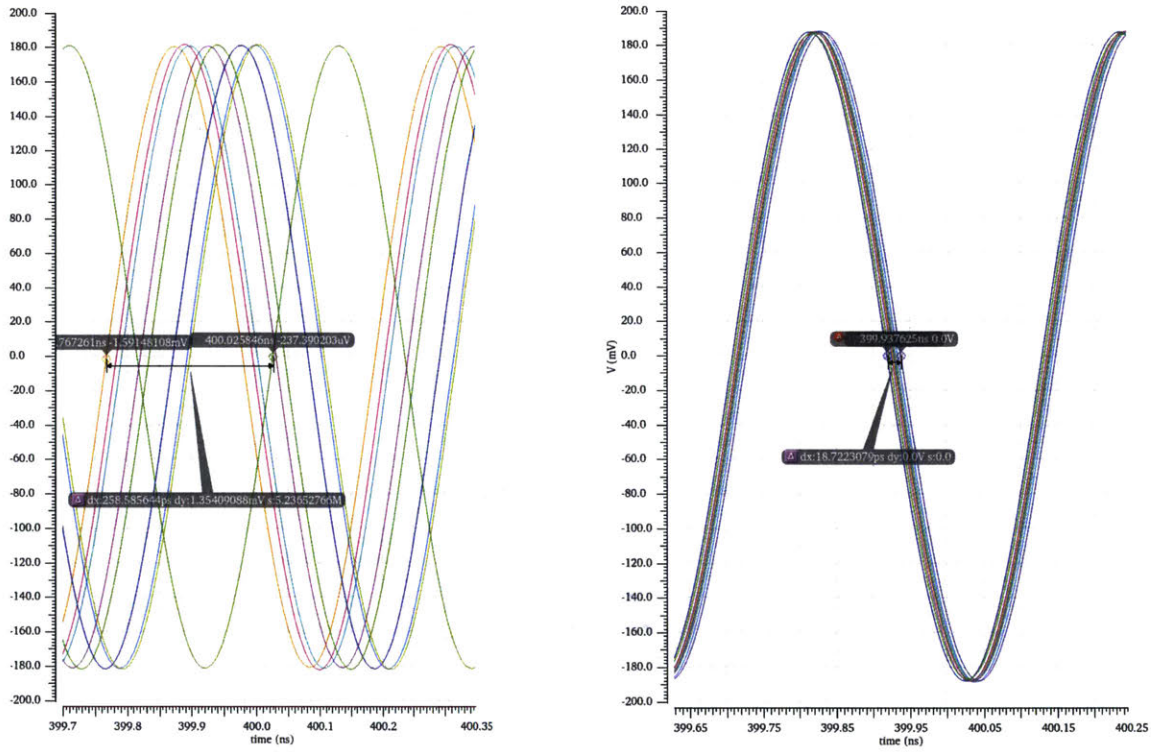


Figure 4-25: LC Oscillator modified circuit for within-bit duty cycling

As mentioned earlier, the datarate of IoT applications is usually low and only requires a few bits to perform a certain task. Hence, another knob to control is the

system's datarate which is here programmed through the bit repetition explained in section 4.7. Figure 4-27 shows a transient simulation for the system at 166 *kbps* with the harmonic rejection within-bit duty cycling scheme employed for power reduction. As shown in the second subwindow, the BPFs can still resolve the the high frequency from the low one and detect the correct bit. This leads to an average power reduction of 33% for the overall receiver which is clear from Figure 4-28 which shows the the supply current in one cycle with almost a few nanoamps at the turn-off time.



(a) Single enable switch startup

(b) Controlled startup switching

Figure 4-26: Overlaid successive oscillation startup waveforms

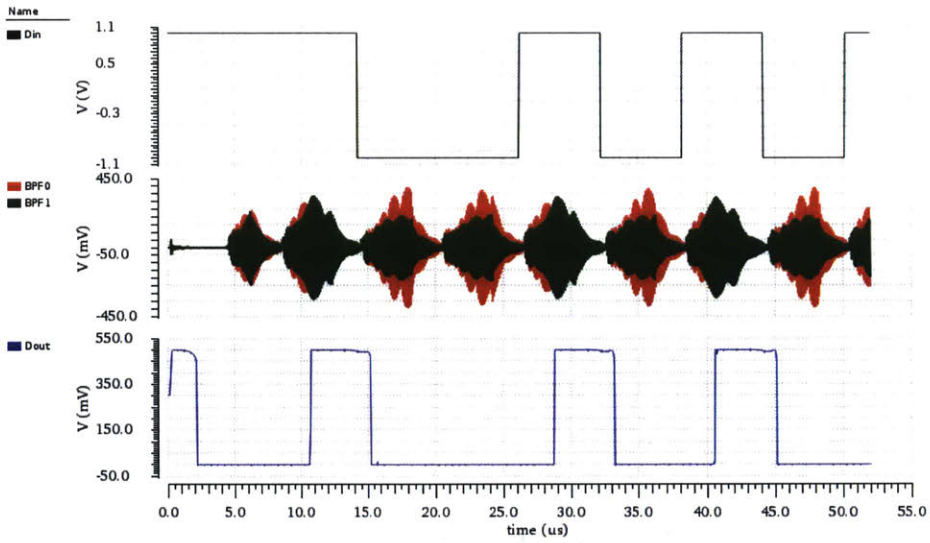


Figure 4-27: Transient simulation of the whole system with within-bit harmonic duty-cycling

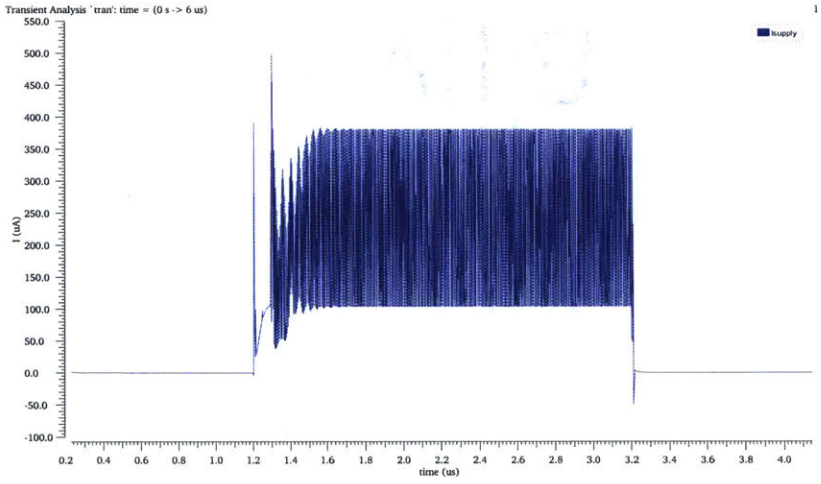


Figure 4-28: One-cycle transient simulation of the supply current with within-bit harmonic duty-cycling

4.10 Layout and floorplanning

The whole chip layout is shown in Figure 4-29 where two replicas of the wake-up receiver are laid out with different frequency ranges for the oscillators to account for any unexpected post-layout frequency shifts.

The floorplanning of the chip aims at isolating the RF circuits from the IF and BB circuits to eliminate any cross-coupling between them. All the RF blocks and interface

are laid out at the left of the block and connected to the left pads of the ring while the lower frequency analog and digital blocks are laid out towards the middle and are connected to the lower, upper and right pads of the pad-frame. Huge decoupling capacitors are added to the supply nodes to stabilize them as much as possible.

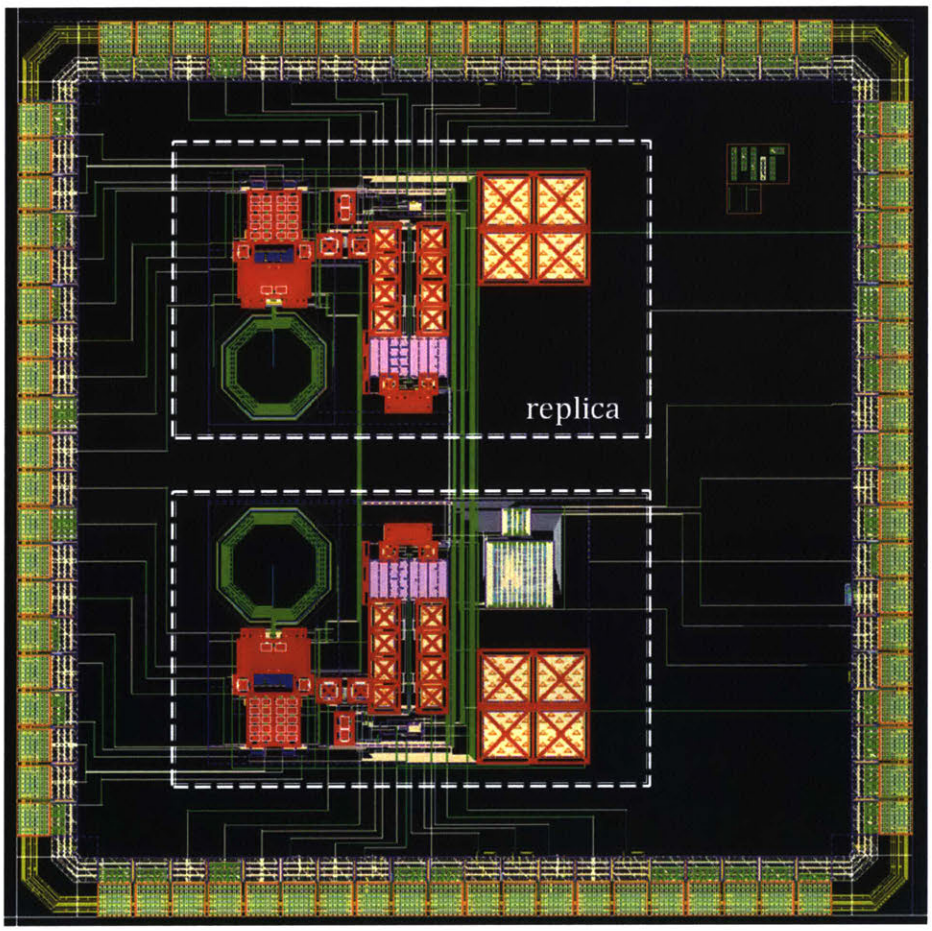


Figure 4-29: Prototype chip layout

Chapter 5

System-level Optimization

In this chapter, system level optimization for the previously discussed circuits are illustrated for a low power secure wake-up communication using conventional BLE advertising packets.

5.1 System duty-cycling scheme

In order to come up with an optimum duty-cycling scheme for ultra low power consumption, then the basestation packet transmission scheme and structure must be analyzed first.

5.1.1 BLE advertising modes

The BLE standard offers four types of protocol data units (PDU) for its advertising packets [34]

- **ADV_IND:** Connectable undirected advertising event.
- **ADV_DIRECT_IND:** Connectable directed advertising event.
- **ADV_NONCONN_IND:** Non-connectable undirected advertising event.

- **ADV_SCAN_IND:** Scannable undirected advertising event.

5.1.2 BLE advertising timing

All undirected events follow an advertising pattern similar to the one illustrated in Figure 5-1 where each advertising event is separated from the following event by an interval $T\_advEvent$ which is given by

$$T\_advEvent = advInterval + advDelay \tag{5.1}$$

where $advInterval$ is the fixed interval between the events given by an integer multiple of 0.625 ms ranging from a minimum of 20 ms up to 10.24 s, while $advDelay$ is a pseudo-random delay ranging from 0 ms to 10 ms determined by the link layer for collisions reduction.

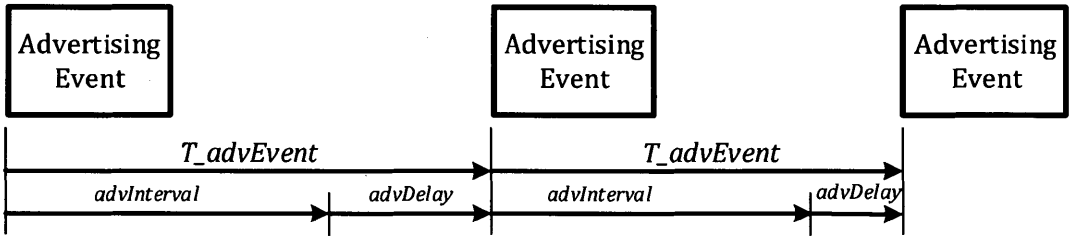


Figure 5-1: Timing of BLE advertising events

5.1.3 Advertising packet format

The undirected advertising packets serve as the best candidate for the IoT wake-up commands as their payload can carry the wake-up sequence of the sleeping node. The packet format is shown in Figure 5-2 where $AdvA$ is the advertiser's address and $AdvData$ is a variable size payload that can hold a user's advertising data up to 31 octets. Thus, these 31 octets can be filled with a repetition of the wake-up sequence

to account for any time misalignment between the wake-up sequence beginning and the packet's least significant bit (LSB) beginning.

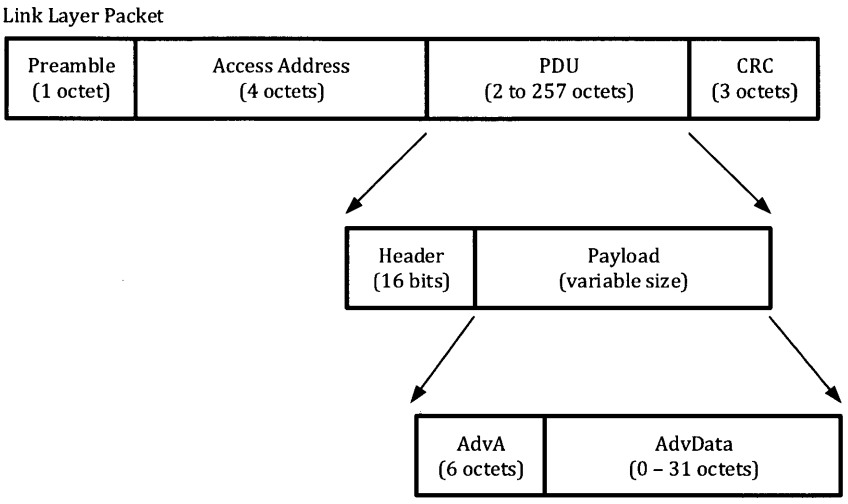


Figure 5-2: Packet format for undirected BLE advertising

5.1.4 Proposed scheme

In order for the wake-up receiver to be able to detect a wake-up event, it has to be active for enough time to guarantee catching at least one advertising packet in the intermittent advertising transmissions. As the advertising event interval is well known, the wake-up receiver active time can be adjusted to be the same which ensures wake-up detection. For instance, if the advertising interval is set to its minimum at 20 ms, then the wake-up receiver active time is set also to 20 ms while the duty-cycling period can be as long as tens of seconds according to the application needs as shown in Figure 5-3.

Therefore, the wake-up receiver's average power consumption can be scaled according to the advertising interval as well as the application's latency. For an active time

of T_{ON} and a duty cycling period of T_{Duty}, the average power is given by:

$$P_{avg} = \frac{T_{ON}}{T_{Duty}} \cdot P_{ON} \tag{5.2}$$

where P_{ON} is the ON power consumed during the active state of the receiver.
The condition which guarantees at least one advertising packet detection then becomes:

$$T_{ON} \geq T_{adv} \tag{5.3}$$

where T_{adv} is the basestation's advertising period.

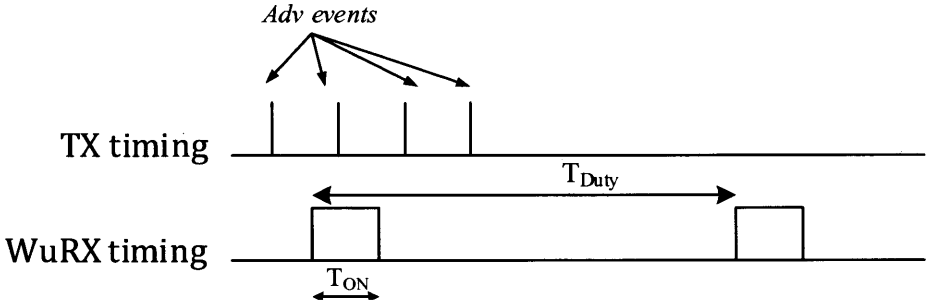


Figure 5-3: Duty-cycling scheme for BLE advertising packets

It is clear from equation (5.2) and Figure 5-3 that if the duty cycling period is allowed to reach tens of seconds then the duty ratio which is the percentage of active power consumed in average can be scaled down to 0.1% of its maximum.

5.2 Security of the Wake-up pattern

With billions of devices being connected together to the internet, the security of the internet and the handheld devices has become both more challenging and more important. In particular, this last year of 2016 witnessed a few cyber attacks all over the world. A distributed denial of service (DDoS) attack on October 2016 brought down a large number of websites for of America's internet for almost a whole day [36]. The attack depends on exponentially increasing the traffic over a server till it collapses

using a huge number of IoT devices with an estimate of 100,000 malicious endpoints. With such a tremendous number of devices and the ease of hacking them, security is becoming a major concern here which even affects the daily life of users.

In the realm of wake-up receivers, the wake-up pattern acts like a pre-shared secret key that can't be compromised. It's the key which opens up a sleeping node to perform any required task.

5.2.1 Fixed Pattern wakeup

The easiest wake-up scheme is to use a fixed wake-up pattern (WuP) where that secret pattern can be exchanged initially with the node before sleeping for the first time through some secure communication. However, as shown in Figure 5-4, if an adversary node is eavesdropping the medium, it can extract this fixed WuP and then use it to attack the wake-up receiver and its sleeping node by draining its battery indefinitely without actual data transmission.

5.2.2 One-Time Pattern wakeup

A scheme which is more resilient to battery draining attacks is one which utilizes a one-time pattern for each wake-up event. Similar to the previous scheme, both the base station and the node can securely exchange a secret key at the very beginning but then then they would use it to generate a new WuP every wake-up event. As shown in Figure 5-5, after using the one-time WuP, both the base station and the node update to a new one for the next event. This means that even if an adversary node is eavesdropping for the WuP and managed to extract it, it wouldn't be able to perform any battery draining attacks as this key is no longer in use.

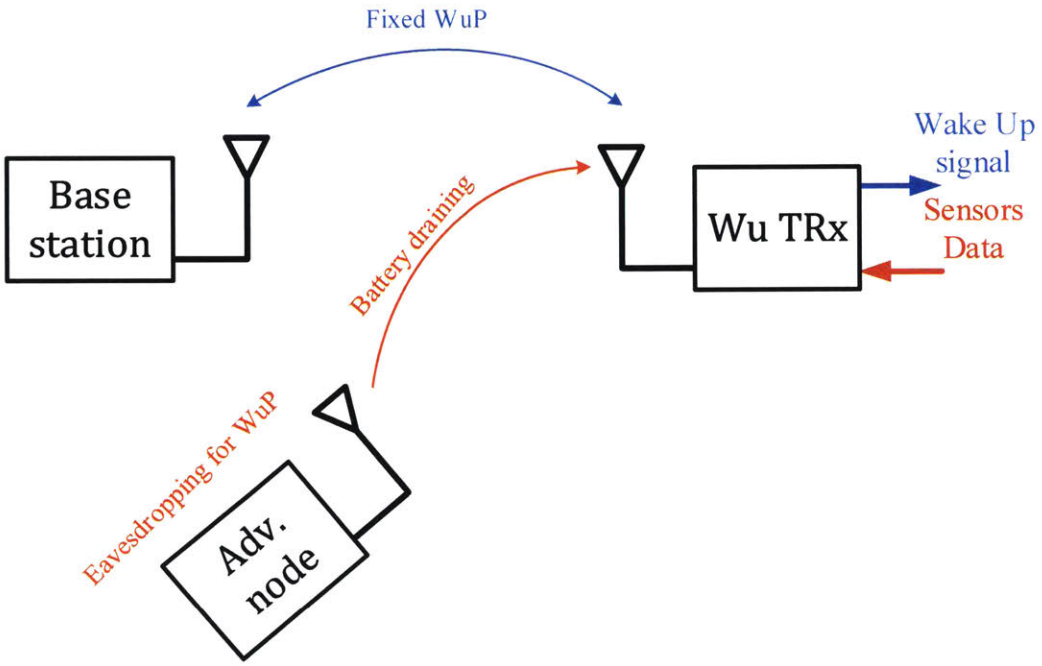


Figure 5-4: Battery drainage attacks in Fixed-pattern schemes

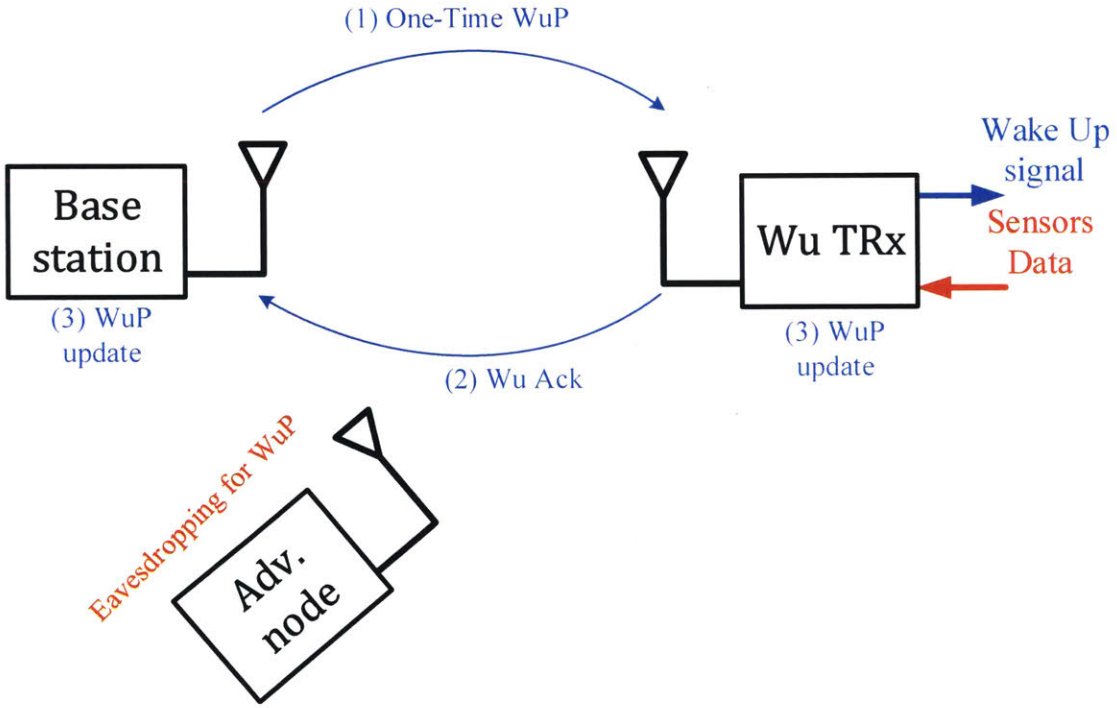


Figure 5-5: Battery drainage attacks in one-time-pattern schemes

5.3 System level results

By applying equation (5.2), it is clear that the shorter the advertising interval is, the lower the average power consumption of the wake-up receiver is. Fortunately, regardless of the advertising interval, there is another knob to reduce the power which is the system latency. Usually, most IoT applications operate at a very low data rate with an acceptable latency of a few seconds. Therefore, the duty-cycling period can be as long as the application allows such that the average power is at its minimum.

A plot of the average power consumption with latency is shown in Figure 5-6 with two different advertising intervals, namely 20 ms and 100 ms. At 20 ms advertising period, the power can be scaled down down to 180 nW at a maximum latency of 20s while at 10s, the average power is almost 370 nW.

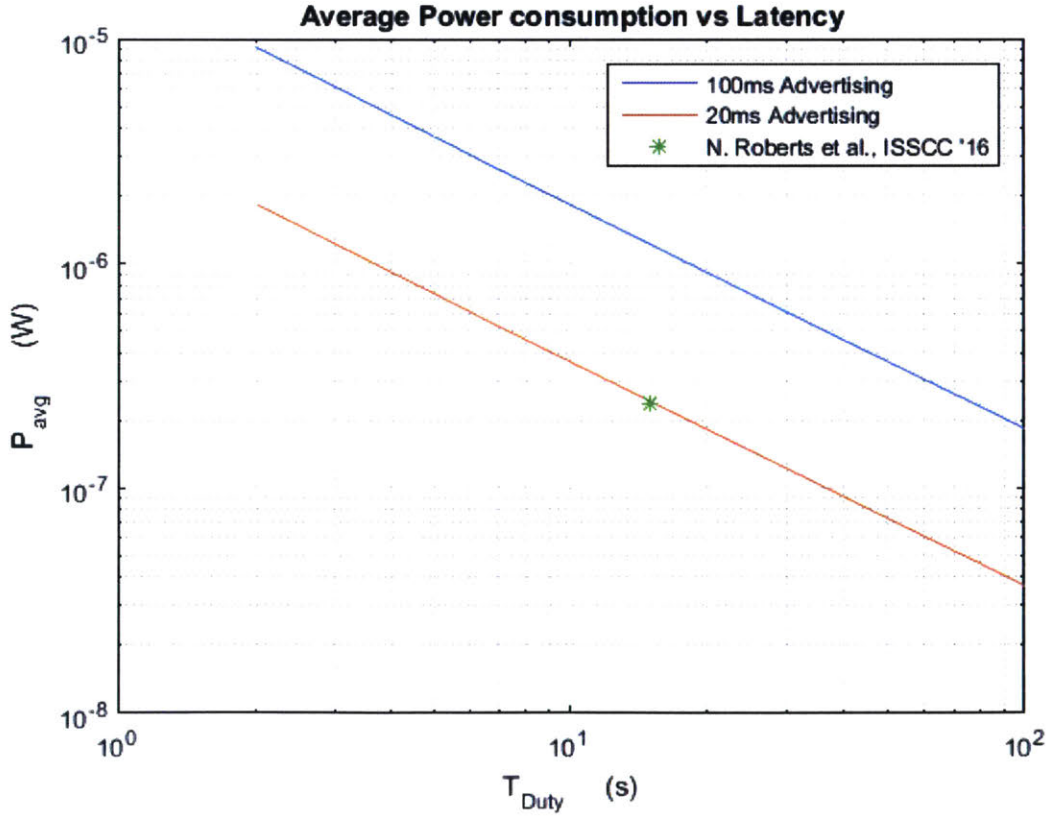


Figure 5-6: Average power consumption with latency at different advertising intervals

Chapter 6

Conclusion and Future work

This chapter provides a summary for the work presented in this thesis and outlines some suggestions for future directions in the area of ultra low power wake-up radio.

6.1 Thesis summary

In this thesis, a new system level analysis for duty-cycled IoT nodes is presented with different trends and optimization directions to determine the datarate and the duty-cycling period. Following that, different ultra-low power receiver architectures are explored for the wake-up receiver system. A new architecture is then developed with high programmability and potentials for an optimized duty-cycling scheme for BLE packets wake-up. A new within-bit duty cycling scheme is proposed with initial phase control in order to achieve 33% power savings while still correctly decoding the input wake-up sequence. The whole system is also duty-cycled with a period which matches the base station BLE advertising interval in order to further reduce the power consumption down to hundreds of nanowatts with almost a 1000× scaling.

A prototype BLE wake-up receiver was built in 65nm CMOS technology. The receiver was designed for a $-90\ dBm$ while new system-level and within-bit duty-cycling schemes are incorporated in the design to reach sub-μW power consumption.

Without an actual connection, the receiver searches the BLE advertising packets for its current wake-up pattern and determines whether to wake-up or not according to the correlation threshold. The receiver operates from a 0.7 V supply and consumes an average power of 1 μW at a latency of $4s$ which can be reduced to 400 nW or even less at a latency of 10 s or more according to the system requirements which depends on the IoT application.

6.2 Future directions

Building on this work, some directions might be explored to improve the system performance as well as efficiency:

- **Wireless Energy Harvesting:** with a low power consumption of 1 μW and below, a wake-up receiver can be operated in a battery-less environment where it is powered by the surrounding environment through some energy harvesting circuitry. It would be quite convenient to have an IoT node which wakes up on Bluetooth packets while being powered using the same packets or through the ubiquitous WiFi packets being transmitted in the air.

- **RF security:** security of the wireless nodes still remains a quite interesting area to explore with lots of potential attacks to be blocked. As the number of nodes keeps increasing exponentially with an explosive amount of data being transmitted, new techniques to improve security in both the RF level as well as the BB level need to be developed.

Appendix A

List of Acronyms

BB: Baseband

BER: Bit Error Rate

BLE: Bluetooth Low Energy

BPF: Bandpass filter

BW: Bandwidth

DC: Direct current

DCO: Digitally controlled oscillator

DDoS: Distributed denial of service

DR: Datarate

FAR: False Alarm Rate

FLL: Frequency Locked Loop

FSK: Frequency Shift Keying

IF: Intermediate Frequency

ILO: Injection Locking Oscillator

IoT: Internet of Things

ISM: The industrial, scientific, and medical band

LNA: Low Noise Amplifier

LO: Local Oscillator

LSB: Least Significant Bit

NF: Noise Figure

OOK: On-Off Keying

PCB: Printed circuit board

PDU: Protocol Data Unit

PLL: Phase Locked Loop

RF: Radio Frequency

RX: Receiver

SNR: Signal to Noise Ratio

TX: Transmitter

VGA: Variable Gain Amplifier

VCO: Voltage-controlled oscillator

WuP: Wake-up pattern

WuRX: Wake-up receiver

Bibliography

[1] IHS-Markit, "Iot platforms: enabling the internet of things." https://www.ihs.com/Info/0416/internet-of-things.html. Accessed: 2016-06.

[2] N. M. Pletcher, S. Gambini, and J. Rabaey, "A 52 μW Wake-Up Receiver With - 72 dBm Sensitivity Using an Uncertain-IF Architecture," *IEEE Journal of Solid-State Circuits*, vol. 44, pp. 269–280, Jan 2009.

[3] C. Salazar, A. Cathelin, A. Kaiser, and J. Rabaey, "A 2.4 GHz Interferer-Resilient Wake-Up Receiver Using A Dual-IF Multi-Stage N-Path Architecture," *IEEE Journal of Solid-State Circuits*, vol. 51, pp. 2091–2105, Sept 2016.

[4] A. Paidimarri, *Circuits and Protocols for Low Duty Cycle Wireless Systems (Can be downloaded at http://hdl.handle.net/1721.1/103674).* PhD thesis, Massachusetts Institute of Technology, Cambridge, 2016.

[5] T. Instruments, "CC2540: 2.4-GHz Bluetooth low energy System-on-Chip." http://www.ti.com/lit/ds/symlink/cc2540.pdf.

[6] Panasonic, "Manganese Dioxide Lithium Coin Batteries: Individual Specifications."

[7] N. E. Roberts and D. D. Wentzloff, "A 98nW Wake-up Radio for Wireless Body Area Networks," in *2012 IEEE Radio Frequency Integrated Circuits Symposium*, pp. 373–376, June 2012.

[8] S. Oh, N. E. Roberts, and D. D. Wentzloff, "A 116nw multi-band wake-up receiver with 31-bit correlator and interference rejection," in *Proceedings of the IEEE 2013 Custom Integrated Circuits Conference*, pp. 1–4, Sept 2013.

[9] P. M. Nadeau, A. Paidimarri, P. P. Mercier, and A. P. Chandrakasan, "Multi-channel 180pJ/b 2.4GHz FBAR-based receiver," in *2012 IEEE Radio Frequency Integrated Circuits Symposium*, pp. 381–384, June 2012.

[10] X. Huang, S. Rampu, X. Wang, G. Dolmans, and H. de Groot, "A 2.4GHz/915MHz 51 μW wake-up receiver with offset and noise suppression," in *2010 IEEE International Solid-State Circuits Conference - (ISSCC)*, pp. 222–223, Feb 2010.

[11] J. Pandey and B. P. Otis, "A Sub-100 μW MICS/ISM Band Transmitter Based on Injection-Locking and Frequency Multiplication," *IEEE Journal of Solid-State Circuits*, vol. 46, pp. 1049–1058, May 2011.

[12] 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.

[13] L. Jae-Seung, K. Joo-Myoung, L. Jae-Sup, H. Seok-Kyun, and L. Sang-Gug, "A 227pJ/b -83dBm 2.4GHz multi-channel OOK receiver adopting receiver-based FLL," in *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, pp. 1–3, Feb 2015.

[14] H. Milosiu, F. Oehler, M. Eppel, D. Fruhsorger, S. Lensing, G. Popken, and T. Thones, "A 3-μW 868-MHz wake-up receiver with -83 dBm sensitivity and scalable data rate," in *2013 Proceedings of the ESSCIRC (ESSCIRC)*, pp. 387–390, Sept 2013.

[15] J. L. Bohorquez, A. P. Chandrakasan, and J. L. Dawson, "A 350 μW CMOS MSK Transmitter and 400 μW OOK Super-Regenerative Receiver for Medical Implant Communications," *IEEE Journal of Solid-State Circuits*, vol. 44, pp. 1248–1259, April 2009.

[16] S. Drago, D. M. W. Leenaerts, F. Sebastiano, L. J. Breems, K. A. A. Makinwa, and B. Nauta, "A 2.4GHz 830pJ/bit duty-cycled wake-up receiver with -82dBm sensitivity for crystal-less wireless sensor nodes," in *2010 IEEE International Solid-State Circuits Conference - (ISSCC)*, pp. 224–225, Feb 2010.

[17] J. Y. Chen, M. P. Flynn, and J. P. Hayes, "A Fully Integrated Auto-Calibrated Super-Regenerative Receiver in 0.13-μm CMOS," *IEEE Journal of Solid-State Circuits*, vol. 42, pp. 1976–1985, Sept 2007.

[18] M. Vidojkovic, X. Huang, X. Wang, C. Zhou, A. Ba, M. Lont, Y. H. Liu, P. Harpe, M. Ding, B. Busze, N. Kiyani, K. Kanda, S. Masui, K. Philips, and H. de Groot, "A 0.33nJ/b IEEE802.15.6/proprietary-MICS/ISM-band transceiver with scalable data-rate from 11kb/s to 4.5Mb/s for medical applications," in *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, pp. 170–171, Feb 2014.

[19] Y. H. Liu, X. Huang, M. Vidojkovic, A. Ba, P. Harpe, G. Dolmans, and H. d. Groot, "A 1.9nJ/b 2.4GHz multistandard (Bluetooth Low Energy/Zigbee/IEEE802.15.6) transceiver for personal/body-area networks," in *2013 IEEE International Solid-State Circuits Conference Digest of Technical Papers*, pp. 446–447, Feb 2013.

[20] B. Otis, Y. H. Chee, and J. Rabaey, "A 400 μW-RX, 1.6mW-TX super-regenerative transceiver for wireless sensor networks," in *ISSCC. 2005 IEEE International*

Digest of Technical Papers. Solid-State Circuits Conference, 2005., pp. 396–606 Vol. 1, Feb 2005.

[21] Z. Lin, P. I. Mak, and R. Martins, "A 1.7mW 0.22mm^2 2.4GHz ZigBee RX exploiting a current-reuse blixer + hybrid filter topology in 65nm CMOS," in *2013 IEEE International Solid-State Circuits Conference Digest of Technical Papers*, pp. 448–449, Feb 2013.

[22] D. C. Daly and A. P. Chandrakasan, "An Energy-Efficient OOK Transceiver for Wireless Sensor Networks," *IEEE Journal of Solid-State Circuits*, vol. 42, pp. 1003–1011, May 2007.

[23] 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.

[24] S. E. Chen, C. L. Yang, and K. W. Cheng, "A 4.5 μW 2.4 GHz wake-up receiver based on complementary current-reuse RF detector," in *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1214–1217, May 2015.

[25] J. Bae and H. J. Yoo, "A 45 μW Injection-Locked FSK Wake-Up Receiver With Frequency-to-Envelope Conversion for Crystal-Less Wireless Body Area Network," *IEEE Journal of Solid-State Circuits*, vol. 50, pp. 1351–1360, June 2015.

[26] M. Zgaren and M. Sawan, "A Low-Power Dual-Injection-Locked RF Receiver With FSK-to-OOK Conversion for Biomedical Implants," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, pp. 2748–2758, Nov 2015.

[27] A. Paidimarri, N. Ickes, and A. P. Chandrakasan, "A 0.68V 0.68mW 2.4GHz PLL for ultra-low power RF systems," in *2015 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, pp. 397–400, May 2015.

[28] X. Huang, G. Dolmans, H. de Groot, and J. R. Long, "Noise and Sensitivity in RF Envelope Detection Receivers," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 60, pp. 637–641, Oct 2013.

[29] C. Andrews and A. C. Molnar, "Implications of Passive Mixer Transparency for Impedance Matching and Noise Figure in Passive Mixer-First Receivers," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, pp. 3092–3103, Dec 2010.

[30] C. Andrews and A. C. Molnar, "A Passive Mixer-First Receiver With Digitally Controlled and Widely Tunable RF Interface," *IEEE Journal of Solid-State Circuits*, vol. 45, pp. 2696–2708, Dec 2010.

[31] M. Lont, D. Milosevic, G. Dolmans, and A. H. M. van Roermund, "Mixer-first fsk receiver with automatic frequency control for body area networks," *IEEE*

Transactions on Circuits and Systems I: Regular Papers, vol. 60, pp. 2051–2063, Aug 2013.

[32] A. Ghaffari, E. A. M. Klumperink, M. C. M. Soer, and B. Nauta, "Tunable High-Q N-Path Band-Pass Filters: Modeling and Verification," *IEEE Journal of Solid-State Circuits*, vol. 46, pp. 998–1010, May 2011.

[33] A. Hajimiri, S. Limotyrakis, and T. H. Lee, "Jitter and phase noise in ring oscillators," *IEEE Journal of Solid-State Circuits*, vol. 34, pp. 790–804, Jun 1999.

[34] "Bluetooth Specification Version 4.2." Bluetooth SIG Standard, 2014.

[35] M. Darvishi, R. van der Zee, E. A. M. Klumperink, and B. Nauta, "Widely Tunable 4th Order Switched G_m -C Band-Pass Filter Based on N-Path Filters," *IEEE Journal of Solid-State Circuits*, vol. 47, pp. 3105–3119, Dec 2012.

[36] "DDoS attack that disrupted internet was largest of its kind in history, experts say." The guardian, accessed at https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. Accessed: 2017-04.