Towards Increasing the Communication Range of Low Power Wireless Devices

By

Yaman Singh Sangar

A dissertation submitted in partial fulfillment of
the requirement of degree of

Doctor of Philosophy
(Electrical and Computer Engineering)

at the

UNIVERSITY OF WISCONSIN–MADISON
2023

Date of final oral examination: 08/01/2023

The dissertation is approved by the following members of the Final Oral Committee:

Bhuvana Krishnaswamy, Assistant Professor, ECE
Paramesh Ramanathan, Professor, ECE
Younghyun Kim, Associate Professor, ECE
Suman Banerjee, Associate Professor, CS
Vaishnavi Ranganathan, Research Scientist, Microsoft Research

To my grandmother, Kamaljeet Kaur
You never truly left, you simply changed form

ACKNOWLEDGMENTS

I would like to express my deepest appreciation and gratitude to the following individuals who have contributed significantly to the completion of this thesis:

First and foremost, I extend my heartfelt thanks to my advisor, Dr. Bhuvana Krishnaswamy. Her support and guidance have been instrumental throughout this research journey. I am grateful for her mentorship, steering me in the right direction and providing me with the space I needed to grow. Her tolerance of my various eccentricities is truly remarkable.

I am immensely indebted to my parents for their unwavering love, encouragement, and belief in my abilities. While I owe my very existence to them, their constant presence and support have been the foundation of every achievement I have seen.

I would like to extend my sincere gratitude to my committee members, Dr. Suman Banerjee, Dr. Parmesh Ramanathan, Dr. Younghyun Kim, and Dr. Vaishnavi Ranganathan. Their valuable feedback has been invaluable in writing my dissertation. I am grateful for the time they dedicated to discussing my research, as well as their assistance in providing access to crucial resources and equipment.

I would also like to acknowledge the contributions of several professors in the department. Dr. Dan van der Weide, Dr. Nader Behdad, Prof. Eric Hoffman, and Prof. Mark Allie have provided invaluable insights, lab resources, and connections to other researchers who have aided my work.

A special thanks goes to my labmates, who created a warm and friendly environment in the laboratory. Yoganand, a collaborator with immense potential, has been a valuable teammate. Osama, a close friend, has been a constant source of company and support. I fondly remember Dan, Manan, Kai, and others who have since graduated, but their contributions remain cherished and remembered.

I express my heartfelt appreciation to the undergraduate students in my lab, including Bhavit, Surya, Ishika, and others. Their constant motivation and infectious energy have been an inspiration, particularly on days that are hard and things aren't working.

To my dear friends Joshua, Aayushi, Jayer, Kyle, Snehal, Shubham, Shruti, and so many others, thank you for being my support system. Your listening ears and presence during moments of venting have been invaluable.

I must also highlight the staff of the ECE department who have always made sure to keep me well-informed and have made the process as smooth as they could. Kathy, Eric, David (Hanke), Katrina, Delight, Amy, and everyone else make sure that we have access to all the resources we need to do the work we want to do.

Finally, I would like to acknowledge that I am here because I stand upon the shoulders of giants. The collective knowledge, guidance, and inspiration provided by the academic community have been instrumental in shaping my research endeavors.

To everyone mentioned above and those who have contributed in various ways, I am sincerely grateful for your support, encouragement, and belief in me. Thank you all for being an integral part of this journey. This would not be possible without you.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The Internet of Things (IoT) technology has been the heart of several technological advances in our day to day. This has been enabled by the seamless connectivity across several types of devices such as wearables, phones, and other sensors deployed across a smart home. Data-driven decision-making is pushing the bounds of connectivity. The scale of devices is increasing, and a higher communication range is desired. However, bulky batteries and power sources deter the deployment of IoT nodes.

In this thesis, I categorize IoT nodes based on the desired communication range: short range up to hundreds of meters, long range up to tens of km, and very long range up to thousands of km. In each chapter of my thesis, I study each of these categories of nodes and propose solutions to achieve a higher communication range without requiring any additional power. I also demonstrate that our novel algorithms are able to accommodate a larger number of devices transmitting concurrently. I present the design and implementation of prototypes built using off-the-shelf (OTS) components. In Chapter Three, I present PACT, a passive battery-free tag with an active radio that communicates with the reader using a novel query-response model to reduce power consumption. Our tag achieves a communication range of 400m and allows for the co-existence of hundreds of tags. In Chapter Four, I present WiChronos, a novel data modulation algorithm that is inspired by optical communication systems. The payload modulated the time interval between two wireless symbols, the preamble and the postamble. Our tag, while coexisting with thousands of other tags, can transmit to a receiver located 4.2km away. In Chapter Five, I present SatConnect, a novel continent-scale IoT node that uses OSCAR satellites to achieve a communication range of thousands of km. Experiments to demonstrate a range of 1100km are being conducted.

1 INTRODUCTION

The Internet of Things (IoT) technology is rapidly emerging as a transformative field that is revolutionizing industries and changing the way we interact with the world around us. IoT refers to the network of interconnected devices, sensors, and objects that can communicate and exchange data seamlessly. From smart cities that optimize energy consumption to wearable devices that monitor health, IoT is shaping a connected world where data-driven insights drive decision-making to improve the quality of life and enhance efficiency, productivity, and convenience[1, 2, 3, 4]. The number of IoT-connected devices was over 10 billion in 2021 and is expected to grow to nearly 30 billion devices by 2030. The total annual worldwide revenue is expected to be over 600 billion U.S. dollars in 2030, nearly a threefold increase from the revenue in 2021 of 213.1 billion U.S. dollars[5, 6, 7]. As the Internet of Things (IoT) continues to evolve, the need for robust and efficient communication networks capable of supporting massive deployments of interconnected devices escalates. The paradigm of enabling large-scale connectivity and communication between an extensive number of machines and devices is referred to as Massive Machine Communication. This involves establishing scalable and reliable infrastructure to facilitate the seamless exchange of data and control signals among a vast array of machines, sensors, and actuators. Through massive machine communication, the vision of a fully interconnected and intelligent world becomes achievable, where machines and devices can communicate, collaborate, and optimize their operations on an unprecedented scale.

However, realizing the vision of massive machine communication paradigm and enable ubiquitous connectivity requires establishing clear requirements for IoT-connected devices. IoT requirements for communication range are spread across a vast spectrum from 10s of meters in

warehouse monitoring applications to a macro scale of 10s of km for smart cities or smart agriculture. Longer range in the order of 1000s of km is desired for remote monitoring of inaccessible sites like deep forest covers or active volcanos. With increasing demands and sensor nodes becoming ubiquitous, the sheer scale of the system poses new challenges on the range, power consumption, and co-existence. Costs of computing have reduced considerably and energy-efficient hardware is cheap and easily available. Achieving long-range and large scale at the cost of increased power consumption results in the need for bulky batteries which is undesirable. To this end, there are three questions that I seek to answer.

1. Can we push the communication range further without increasing the overall tag power consumption?

2. Is it possible to do it using OTS devices?

3. Is it possible to do it at scale to enable co-existence?

To answer these questions, it is important to understand the reasons behind the scale and range limitation of low-power IoT nodes. As a system scales up, multiple devices transmit concurrently. This leads to packet collisions resulting in potential loss of data and resources. To prevent this, Time Domain Multiple Access (TDMA) is a popular choice for most low-power wireless technologies. TDMA is a technique where several nodes share the frequency channel by transmitting in time slots defined for each node. The larger the number of nodes, the larger the latency to receive from these nodes. Therefore, when we envision systems that scale significantly, much beyond the limits of current state-of-the-art technology, we require newer solutions that enable these nodes to transmit concurrently. The second limitation stated above is the range. The maximum range that a wireless front end can achieve is a function of the path loss in the operational spectrum, transmit power, and hardware/software gains

of the system. Path loss defines the attenuation faced by the electromagnetic signal in traveling through a medium (air) and is constant for a given distance. FCC regulates the maximum allowed transmit power at various frequencies. Techniques such as spread spectrum modulations or ultra-narrowband modulations are used to achieve a better range. Spread spectrum modulations increase the SNR of the received signal through the processing gain of the system (the ratio of transmission and data bandwidth). Ultra-narrowband modulations reduce the receiver bandwidth in the order of a few kHz. Reducing the bandwidth also reduces the overall noise power and therefore, reduces the noise floor at the receiver. This reduction in the noise enhances the Signal Noise Ratio (SNR), thereby increasing the range. However, all of these techniques require substantial power. In order to achieve low power consumption, the current state of the art limit either the time period for which these nodes can transmit or put limitations on the overall size of the payload that can be transmitted. A key observation I make here is that even though these nodes are capable of transmitting at a high data rate, the overall data rate achieved on a macro timescale (over a period of 24 hours for example) is low. In other words, these technologies have been engineered to provide solutions for IoT connectivity by putting appropriate limitations on existing technologies rather than approaching them as a fresh set of problems. In my thesis, I propose and implement techniques to achieve long-range and large scale at similar or lower power consumption by trading off the data rate. The payloads of these nodes are usually small pieces of data captured by sensors and hence, these nodes do not require a high data rate. I design all the prototypes using off-the-shelf components such as low-power microcontrollers, radio, FPGA, and software-defined radios. All PCB files and other software have been made available publicly and more information on this is available in the following chapters.

To that effect, I define three categories of devices and present the con-

tribution this thesis makes toward each of these categories. I propose categorizing IoT devices on the basis of communication range: short range, long range, and very long range. I do so because these categories share similar characteristics like power consumption, scale, and data rate. Short-range IoT devices consume the least amount of power range in the μW range. These devices can be passive or battery-less and in order to enable passive operation, they do not use a radio front end. Energy is harvested from RF signals or other sources like solar or piezo. They rely on RF signals from a dedicated source (or ambient signals) to send to a receiver. The communication range achieved by these devices ranges from 10s to a few 100s of meters. For example, RFID technology has both active and passive tags and these are widely used in monitoring and tracking applications. The long-range category of IoT devices consists of devices that consume several mW to 10s of mW of power. Small coin cell batteries that last for a few years are often used, though it can be augmented with harvesting to charge the batteries. These devices achieve a communication range of 100s of m to several km. Some examples include LoRa, Sigfox, and NB-IoT. These are often used in sensing applications to enable smart agriculture and smart cities. Finally, the very long-range category consists of devices that consume 100s of mW of power and require larger batteries or even a continuous power supply. These devices are capable of higher power transmissions and achieve ranges in the order of 100s to 1000s of km. For instance, Starlink, Swarm, and Lacuna provide nodes that are capable of transmitting to one of the satellites in their private constellations. These devices are ideal for monitoring dangerous locations like active volcano sites or deep forest covers that are hard to reach.

In my work, I rethink communication algorithms for each of these categories of tags and propose, implement, and prototype solutions toward pushing the limits of the communication range. I identify that a 'one solution fits all' approach doesn't work because though each category

has similar requirements, the goals for each category are different. Short-range IoT devices are often batteryless and energy efficiency is important. Long-range IoT has stricter requirements on range but low data rates are acceptable. Very long-range IoT is very expensive and low-cost means to achieve it are required. With these goals in mind, I make the following contributions:

- Short range (a few hundred meters, less than 1km): I propose the design of a passive tag (PACT) that harvests RF energy and uses an active front-end radio to respond. A query-response algorithm is implemented so that 100s of tags can transmit concurrently. PACT improves the range of battery-less devices that belong to the first category of wireless devices identified above. Off-the-shelf low power microcontroller and radio are used to implement the tag and all the source files are made available publicly to enable easy access to build and use the tag.

- Long range (a few km to tens of km): I design and prototype a wireless tag (WiChronos tag) that modulates data in the time difference between two short wireless symbols, a preamble and a postamble. Off-the-shelf radios are used to transmit ultra narrowband FSK or chirp-based preamble and postamble. Low-power microcontrollers with accurate clocks are used to modulate data. By maintaining the IoT node in low power mode during the time between the preamble and postamble and thereby, sending information while remaining silent, WiChronos reduces the power consumption without compromising on the communication range. Preambles and postambles can be interleaved while other devices are actively sending data to achieve better scalability. Off-the-shelf radios are used to implement WiChronos and the circuit connections, block diagrams, and other files are made available publicly.

- Very long-range IoT: With an intent to democratize available resources like LEO satellites, SatConnect uses chirps to transmit data through existing amateur satellite networks. This reduces the costs associated with very long-range IoT devices in launching satellite clusters and building ground stations. The transmitter and receiver are implemented using off-the-shelf software-defined radios. All the hardware like antenna, amplifiers, and modulation and demodulation software is available publicly.

It must be noted that the solutions I propose are cross-layer approaches where I use information and knowledge from the application layers to inform optimizations in the physical and link layer of the communication stack. Therefore, there aren't neat distinctions across these layers. While there are several examples of other cross-layer approaches that I explain further in Chapter 2, these solutions rely on existing hardware infrastructure like WiFi. However, using edge computing tools provides us the capabilities to explore such a cross-layer solution space. Therefore, exploring these ideas would not have been as straightforward a few years ago but we now have the capability as well as the need for them. By using information from the application layer in designing the physical and link layer, we are able to reduce the energy consumption of the devices and enable better scalability.

The rest of the dissertation is organized as follows: In Chapter 2 I present a survey of the literature and state-of-the-art wireless technologies used for IoT nodes across a variety of scales and power consumption. I compare the communication range and power consumption of these technologies and identify gaps where new solutions are needed. In the next Chapter 3, I present my work titled PACT where I explain the design of a batteryless tag that harvests RF energy to respond to queries from the reader. A novel query-response algorithm is implemented to reduce power consumption, and the use of an active radio enables us

to control the center frequency of each tag, thereby increasing the scale of the system to 100s of devices. In chapter 4 I present my work titled WiChronos where I introduce a time interval modulation technique for data transmission. I demonstrate that while consuming lower power than state-of-the-art, the implemented prototype achieves a range of several kilometers while reducing the spectral usage leading to the ability to accommodate a larger number of devices. In chapter 5, I present my work on an IoT communication system leveraging OSCAR satellites to enable IoT devices to communicate across a range of several thousands of kilometers. Finally, I conclude my work and discuss several next steps in Chapter 7.

2 LITERATURE SURVEY

Since the 1980s, every decade has seen a new generation of wireless technology. The first generation of cellular networks used frequency modulation across a 30kHz bandwidth and used FDMA to support multiple devices. The second generation saw the bandwidth raised to 200kHz and used Gaussian minimum shift keying (GMSK) modulation. TDMA was used to support multiple devices. 2G devices attained low power consumption that aided in prolonging the battery life and this became a tipping point in wireless research. 8PSK was also introduced as an alternate modulation technique that provided a higher data rate but a lower communication range. By the third generation, a bandwidth of 2.6GHz was assigned for cellular networks where a combination of wideband code division multiple access (W-CDMA) and high-speed packet access (HSPA) was used for internet access and media streaming. By the 4th and the 5th generation, the bandwidth increased to 20MHz and 100MHz respectively. Cellular networks are currently exploring 6G technology to meet the demands of data, latency, and connectivity. In fact, one of the use cases of 6G is massive machine-type communication (mMTC). mMTC is a type of communication between machines that requires little to no human intervention and is one of the building blocks of the Internet of Things (IoT) infrastructure. IoT devices and sensor networks find applications in several domains from wearable devices, healthcare, and automation to smart agriculture, smart cities, and security. These technologies have emerged from a variety of research and industry endeavors and form a significant portion of current research to advance wireless research. Several existing techniques/technologies like backscatter[8, 9, 10, 11, 12, 13, 14, 15, 16, 17], RFID[18, 19, 20, 21], bluetooth and bluetooth low energy (BLE)[22, 23], LoRa[24, 25], SigFox[26], NB-IoT[27], and Zigbee[28], Lacuna[29], Swarm[30], and Starlink[31] are used in IoT and sensor networks. In the rest of this chapter, I will

explain these technologies, their pitfalls, and the existing challenges.

A large number of low-power wireless data transfer techniques rely on using backscatter to transmit a payload. Backscatter is a type of wireless communication technology that enables devices to communicate by reflecting existing signals rather than generating their own. The general setup of a backscatter-based system consists of the tag, an excitation source that provides a high-power continuous wave, and a receiver. The tag encodes bit '0' by absorbing the excitation signal and bit '1' by reflecting the excitation signal toward the reader. The reader perceives bit '1' upon receiving the reflected excitation signal from the tag and bit '0' when no such signal is received. Radio Frequency IDentification (RFID) tags[18, 21] use the principle of backscatter to communicate with the reader and are widely used in several applications like tracking and monitoring. An RFID reader[32, 33]r is capable of transmitting the high-power excitation signal as well as receiving the low-power backscatter signal from the tag. As a result, it employs sophisticated hardware for self-interference cancellation. The tags can be passive, meaning they do not have a battery and are charged by harvesting RF power from the excitation signal or active, meaning that they are powered by a battery. Passive tags usually have a maximum range of 10m whereas active tags can achieve a range up to 30m. Wireless Identification and Sensing Platform (WISP)[17] is another well-known platform for backscatter research. The principles of WISP like Dickson charge pump for harvesting, a low power envelope detector-based receiver, and backscatter to relay the payload have inspired many research endeavours[34, 35, 36, 37].

Backscatter that utilizes pre-existing infrastructure as the power source, as well as excitation signal for the tags, has been of much interest in academia. Several technologies also shift the frequency of the reflected tag signal from the excitation signal frequency to reduce/omit interference. FM backscatter[10] uses ambient FM signals in the environment to

harvest energy from as well as communicate to a reader. Locations that are close to cellular towers are particularly good locations for these tags where they are able to backscatter payloads on ambient signals of as high as -30dBm power. FM backscatter tags suffer from a restricted communication range of 60 feet. Further, RF harvesting efficiency at such power levels increases the charging time and limits the application scope considerably. Several current commercial solutions [38, 39, 40, 41, 42, 43] utilize Bluetooth-Low-Energy (BLE) enabled real-time monitoring. However, the short life and bulkiness of batteries needed for BLE poses a challenge and is not sustainable at scale. BLE backscatter[23] leverages signals from existing Bluetooth infrastructure as the excitation to backscatter on. BLE backscatter devices may be as much as 30m from the source and consume 1.56nJ per bit transmitted. The low energy consumption enables battery-free operation, though it is limited when the payload size increases. They can communicate with a reader that is up to 1m away. HitchHike[44] uses WiFi signals from a commodity 802.11b WiFi transmitter to backscatter to a reader. The tag shifts the frequency of the transmitted signal to prevent self-interference without using an oscillator to keep it extremely low power and enable passive operation. Additional hardware is required at the receiver to decode the packets. Further, the latency of a HitchHike tag increases in trying to remove destructive interference. The tag is able to achieve a communication range of 54m in LOS conditions while consuming 40mW of power. An IC implementation can bring down the power to 33μW. Xshift[14] utilizes unique leakage characteristics of off-the-shelf (OTS) hardware to decode the payload as well as allow for multiple devices to co-exist. It still suffers from the dual path loss problem of backscatter which limits the range. More importantly, using different hardware where nonlinearities are lower will render the technique unusable. Though Xshift is a step towards marginally better scalability, the communication range it achieves is 2.4m and the tag consumes 48.1μW. An IC implementation can

bring the power consumption down to 6.8μW.

Another stream of research has been focused on amalgamating spread spectrum techniques and backscatter by leveraging LoRa infrastructure[45]. Currently, LoRa has a market value of USD 5.6 billion and it is projected to reach USD 25.5 billion. Further, Chirps offer the advantage of a longer communication range due to the spread spectrum gain. pLoRa[12] uses passive tags that rely on packets being transmitted by an active LORa node to act as the excitation source. This backscattered signal is received by a LoRa receiver which is able to demodulate and decode the data. LoRea[13] on the other hand relies on ambient LoRa signals as the excitation. Therefore, pLoRa achieves a communication range (tag to receiver) of 1.1km with the tag being separated from a LoRa node by a maximum of 20cm whereas LoRea achieves an impressive 3.4km range so long as the tag is less than 1m from a LoRa node transmitting at 28dBm power. A pLoRa node consumes 220μW whereas a LoRea node consumes 70μW of power.

It must be noted that these approaches toward better energy efficiency rely on the presence of existing infrastructure that is assumed to be ubiquitous. However, this assumption is true often only in urban environments. Technologies that rely on the presence of LoRa and WiFi can only modify packets specific to these technologies to send their payloads. It is because of the fact that we have better computing resources as well as the ubiquitous nature of WiFi, Bluetooth, and such technologies that we have the capability to explore alternative ways of leveraging them. This is a new solution space that may not have been possible to investigate a decade ago; only now is there the capability as well as a need to delve into it further.

Though backscatter techniques decouple carrier generation and transmission, they still send all the bits of the payload to the reader and maintain a clear distinction between the application layer and other layers of the communication stack. Improvements in technologies such as edge computing and machine learning enable us to blur the neat lines of the communication

stack and explore cross-layer protocols. It is possible to draw inferences from the application layer and use it to optimize the physical or link layer for better energy efficiency, easier deployment, or even to leverage existing infrastructure. Various cross-layer approaches have also been proposed [46, 47] to optimize communication and analytics for power consumption. Battery-free cellphone [47] reduces power consumption by using backscatter and analog electronics for transmission and reception. Analog speech data encoded in the RF transmissions actuate the headphones on the receiver. Wispcam [46] uses a charge-storage model where the leakage energy during the charging cycle is used as a cost function to optimize the capacitor use during the active cycle. Backscatter communication and fast nonvolatile memory enable quick transfer of the camera image to a nonvolatile memory before exhausting the capacitor's supply. These techniques use the requirements from the application layer to optimize power consumption to enable battery-free operation.

These backscatter approaches discussed here rely on low power tags so that a small battery is sufficient if even needed. To achieve longer ranges, the power consumption of the tags increases. Several solutions such as LoRa, NB-IoT, SigFox, and Zigbee have been proposed and are widely used. These technologies that use low power tags and achieve long communication ranges are referred to as Low Power Wide Area Network (LPWAN) technologies. Lora[24] uses chirps to modulate data which offers the advantage of spread spectrum gain. Hence, LoRa has been shown to achieve ranges of up to 20km in rural settings and 5km in urban spaces. NB-IoT[27] uses FSK at a narrow bandwidth of 120kHz. Reducing the bandwidth also reduces the noise floor and hence, enhances the SNR of the received signal which translates to longer ranges of up to 12km. SigFox[26] operates at an ultra-narrow bandwidth of 0.1kHz and achieves a communication range of up to 17km. Zigbee[48] uses BPSK at the 915MHz frequency range and OQPSK at 2.45GHz. It achieves a range

of up to 100m. Though all of these technologies achieve long range, none of the tags are inherently low power consuming. In fact, energy efficiency is achieved through duty cycling - limiting the frequency at which the payload can be transmitted or simply putting a cap on the number of transmissions allowed.

Long communication range of up to 50m is also achieved by cellular networks[49]. Orthogonal Frequency Division Multiplexing (OFDM) modulation technique in cellular networks enables a large scale of thousands of devices to transmit concurrently[49, 50]. Though the costs of using cellular devices are reducing, the power consumption is in the order of several Watts.

LPWAN and cellular technologies are able to increase the range of IoT devices to 10s of km. However, several applications that require sensors to be placed in remote locations also require connectivity. To address this need, satellite IoT is an emerging field now, and has gathered interest in academia as well as industry. Several companies like Lacuna, Starlink, and Swarm are now launching their own satellite clusters and offer sensor nodes that can be bought. These companies also offer various plans depending on the frequency and amount of data to be transmitted. Lacuna[29] relies on LoRa as the modulation and has launched 6 out of 240 planned satellites. Swarm[30] has launched 189 satellites so far and the company has been acquired by Starlink recently. Starlink[31] uses QPSK and BPSK for downlink and uplink paths respectively and currently has over 4500 satellites in orbit. All these technologies require substantial infrastructure and money to launch satellites and build ground stations.

I seek solutions that are not dependent on new or better hardware but a more efficient means of using available hardware. I propose solutions to increase the range of batteryless as well as battery-powered devices by using approaches across multiple communication layers to achieve the goals of low energy and large scale at long range. The next 3 chapters in

this thesis address a different realm of technology and propose means to increase the communication range and scale. In Chapter 3, I present my work titled PACT where I propose the design and prototype of a passive tag along with a query-response communication algorithm with the reader aimed at increasing the communication range and allowing 100s of tags to respond concurrently. I use the knowledge available to us from the application layer to optimize power consumption on the tag and compare the effectiveness of PACT against backscatter. PACT saves the energy expended in transmission at the same bandwidth as backscatter by eliminating the need to send every bit of payload. In Chapter 4, I discuss my work titled WiChronos where I propose a time interval modulation technique to achieve a communication range in the order of several km while maintaining low power consumption. This is directed as an alternate solution toward LPWAN technologies where I demonstrate that WiChronos is able to increase the communication range and the system scale without compromising on energy efficiency. WiChronos effectively sends data when the devices are in deep sleep mode, thereby saving power. Finally, I present SatConnect in Chapter 5 which is aimed towards democratizing the use of existing satellites to achieve connectivity with devices that are separated by 1000s of km from a ground station. By using existing satellite clusters, SatConnect reduces the costs associated with very long-range IoT communication.

3 PACT: IMPROVING THE COMMUNICATION RANGE OF BATTERYLESS WIRELESS TAGS USING ACTIVE RADIOS

3.1 Introduction

Data-driven optimization is slowly revolutionizing various industries. This, however, calls for pervasive sensing to generate the necessary data, which has so far been led by the evolving technologies in IoT. For example, humidity and temperature control in food and dairy industry is a crucial topic of academic and commercial significance due to the industry's direct impact on economy and the health and safety of consumers [51, 52]. Roughly one third of current global fresh produce is thrown away; a bulk of it is due to non-optimized post harvest handling and storage losses that are estimated between 0.5% - 10%[53, 54]. The perishable goods transportation market, which is expected to register a growth of $6.43 billion in the next 5 years[55], is a critical point for such smart monitoring to reduce food loss. Over the years, the Food and Drug Administration (FDA) has implemented strict regulations on humidity and temperature (quality) control in the food supply chain to prevent the spread of food-borne illnesses. However, the actual implementation of such sensing and traceability is a work in progress as technology evolves to meet strict cost requirements. The FDA's follow-up initiative on "Smarter Food Safety" explores low-cost technologies to quickly trace a food product throughout the system to prevent large-scale spread of food-borne illnesses and retain nutrition of food products [56, 57]. This ability to track and discard "bad apples" quickly also has a significant impact on the economy [51, 57, 58]. Keeping the sensing cost low at large scale is crucial in the food industry due to the already low profit margins. A number of startups and commercial stakeholders that utilize cloud-based IoT platforms [38, 39, 40, 41, 43, 42] have emerged to deliver smarter food safety. most of the monitoring is still

manual, prone to error, and does not scale. Simple, low-cost sensing and tracking in real-time with data storage from a large-scale of food products remains an open challenge [59].

The key requirements for practical implementations of such large-scale, low-cost monitoring systems are,

- Low-power and low-complexity network: In the case of a large number of low-power sensors deployed for data-driven applications, there is a need to keep the technology environmentally sustainable.
- Long-range and scalable communication: Specifically in the agriculture and food industry, the communication range of sensing can be over hundreds of meters, such as across warehouse/fields. Being able to easily communicate with multiple sensors in real time is crucial for process and cost optimization.
- Low-cost and long battery life at scale: With the low profit margins of the global food industry, keeping the monitoring and maintenance costs low with long battery life helps easy adoption of the technology.

While Bluetooth-Low-Energy (BLE) is popular among commercial solutions [38, 39, 40, 41, 42, 43], backscatter communication is an emerging alternative technology to address the low-power and low-cost needs of monitoring applications [60, 61, 17, 11, 44, 16, 62, 63, 64]. However, since information is conveyed by scattering back existing signals, the communication range of traditional backscatter systems is constrained, limiting practical deployments [11, 44, 16, 10]. We identify three key reasons for the **short range** of a passive backscatter system:

RF **Energy harvesting range** to power the tag,

Reader sensitivity in receiving the backscattered signal in the presence of self-interference from the excitation signal,

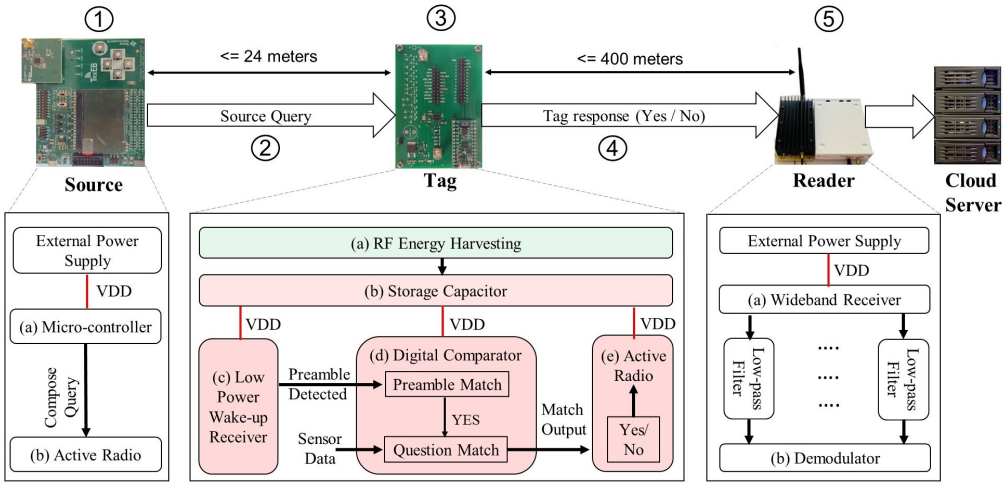


Fig. 3.1: PACT framework. ① Source, a transmit-only active radio ①b, broadcasts the Query at 14dBm to the Tag. ② Source Query supplies power to the Tag and asks a specific Question for the Tag to compare. The harvesting range of PACT determines the maximum distance between the Source and the Tag. ③(a) RF harvesting unit on the Tag stores energy on the ③(b) 6.8µF storage capacitor and supplies power to the ③(c) low power wake up receiver, ③(d) FPGA, and ③(e) the AX5043 active radio on the Tag. The wake up receiver detects the Preamble and Question which are compared digitally on the FPGA and the output of the Question match triggers the active radio. ④ Tag response from the active radio transmitted at 0dBm is FSK modulated with 15kHz BW at 1.2kbps baud rate and a 2dBi whip antenna. (5) Reader with a sensitivity of -95dBm to support 400m communication range receives Source Query and the Tag response. It uses a 25 dB gain power amplifier. The wideband USRP receiver ⑤(a), using digital filters, receives Tag response from multiple channels ⑤(b) and relays it to cloud.

Dual path loss faced by the backscattered signal. While research on energy-harvesting [65, 66] and alternate architectures [9, 67, 12, 68] have addressed (1) and (2), dual path-loss is an inherent characteristic of backscatter due to the distance traversed by the backscattered signal [69]. The limited range due to dual path loss in turn demands the use of more readers to communicate over larger areas, which affects scalability. Hence,

backscatter-based systems do not meet all the needs of large-scale, low-cost monitoring systems.

In this work, we propose PACT (Passive communication with ACTive radio), a scalable communication system that improves the energy efficiency and communication range of battery-less Tags by leveraging the knowledge asymmetry in monitoring and tracking systems. Consider a smart temperature monitoring system in a food storage unit, where each product is sensitive to a certain range of temperature. A food safety concern arises when the temperature is outside its sensitive range [70, 71]; which is typically known apriori [72, 73]. PACT leverages this prior knowledge and designs the Source to send a specific Query, which has the dual purpose of powering the Tag as well as querying the Tag. As illustrated in Figure 3.1, our proposed system consists of a Source ❶, a Tag ❸, and a Reader ❺. A PACT Source is an RF excitation source that broadcasts a Query ❷ using an active radio transmission. The Source Query is designed to power the battery-less Tag, which harvests energy from the Query itself. It also includes specific questions to the Tag e.g., "*Is the temperature below 30 F?*". A PACT Tag compares the sensor data with this Question and responds with a *yes* or a *no* using an active radio ❹. A PACT Reader listens to the Tag response, and uploads it to a cloud server. **A PACT Tag, thus, improves the communication range by transmitting a short yes/no response using an active radio, while still operating only on energy harvested from the Source query, rendering the Tag battery-less.**

Although the yes/no responses are short and consume lesser energy than sending the actual sensor data, the active radio is energy-consuming. In order to power this active radio, we design an energy harvesting circuit to maximize the harvesting range and efficiency. Additionally, the Q&A format of PACT provides the desired flexibility for monitoring and tracking systems to ask different questions (frame different queries) for different products and environments. Finally, offloading the data encoding to the

Source through queries simplifies the Medium Access Control (MAC), one of the major challenges in practical deployments of RFID [74, 75]. PACT network is divided into Tag groups, where the Source queries all the Tags in a Group using their Preamble. Each Tag concurrently responds in a unique channel (up to 520 channels with 15kHz BW) in the 902-928 MHz band, leveraging Frequency Division Multiple Access (FDMA). As the network grows, new groups with distinct Preambles are created and queried sequentially. By leveraging Time Division and Frequency Division Multiple Access, PACT allows hundreds of Tags to co-exist and the network to scale without affecting latency or energy efficiency. **We perform real-time evaluations to show that a PACT Reader can communicate with an estimated 520 battery-less Tags in a single group placed at distances of up to 0.4 kilometer concurrently.**

In summary, we leverage the knowledge asymmetry in monitoring and tracking systems to query Tags that respond with a yes or no, towards realizing a scalable, low-cost, and long-range communication network of battery-less Tags. Specifically our contributions are the following:

- We propose a scalable, ultra-low-power communication paradigm that uses prior knowledge at the excitation Source to Query a battery-less Tag that harvests RF energy from this query. Our proposed Tag consumes energy as low as 23μJ for its operation. This includes the energy consumption of an active radio on the Tag that improves the communication range of the passive Tag to nearly 400 meters.PACT combines the strengths of active radio communication and passive tags operating on harvested energy.

- We design a custom energy harvesting front end to enable battery-less operation of a PACT Tag. We design an ultra low power envelope detector and a digital comparator to demodulate and decode the Query from

the Source. We implement and experimentally verify the RF energy-harvesting circuit that powers the PACT Tag.

- We propose and implement a hybrid Time-Frequency division MAC to allow the co-existence of large scale of Tags avoiding collisions and reducing network latency compared to state-of-the-art. We show that a group of 520 Tags can communicate with one Reader concurrently, increasing the network throughput.
- We prototype a PACT Source, Tag, and Reader using commercial off-the-shelf (COTS) components on a PCB and experimentally demonstrate an RF energy-harvesting range of 24 meters to operate a Tag that consumes 23μJ energy, and achieves a communication range of over 400 meters.

The rest of the chapter is organized as follows: section 3.2 presents an overview of PACT system design. In section 3.3, we present in detail the Source Query design, Tag Design, Tag Response, and expected throughput of PACT. In section 3.4, we propose a hybrid MAC protocol that allows PACT to scale and Tags to coexist in a network, followed by section 3.5 where we describe our implementation, hardware, and settings used. section 3.6 evaluates the range, energy, latency, and coexistence performance of PACT. We identify use cases of PACT in section 3.7, and related works in section 3.8.

3.2 An overview of PACT system design

The goal of this work is to develop a communication paradigm that can address the low-cost, long-range, and large-scale needs of real-time monitoring systems. Building on top of low-power backscatter communication principles, we design and prototype PACT, a communication system that leverages knowledge asymmetry to improve the range of a large-scale network of battery-less Tags. PACT is particularly useful in applications

where it is critical to understand the range of data and not its absolute value.

As illustrated in Figure 3.1, our proposed system consists of a Source, a Tag, and a Reader. The Source is a transmit-only active radio, that broadcasts an Amplitude Shift Keying (ASK) Power-up sequence (train of bit 1s) followed by an ASK modulated Query. The Tag harvests energy from the power-up sequence. On harvesting sufficient energy from this sequence, the Tag wakes up, listens, and demodulates the Query from the Source using an envelope detector. It then compares its sensor data with the received Query and responds with a *"yes"* if there is a match, and a *"no"* otherwise. The Reader is a simple receiver that listens to both the Query from the Source and the Tag response. The Tag response is transmitted using an active radio and faces only one-way path loss from the Tag to the Reader; the active radio avoids the dual-path loss and thus overcomes the range limitation of backscatter. The communication range of a PACT Tag, therefore, depends only on the distance between the Tag and the Reader and the Tag's modulation characteristics. The improved communication range of PACT allows us to deploy a single Reader to communicate with hundreds of Tags concurrently. We design a 3-node architecture with a decoupled Source and a Reader to simplify the infrastructure and reduce costs. Source being a transmit-only radio that broadcasts ASK modulated queries, can be battery-powered and low-cost as it goes to low-power sleep mode between queries. The Reader on the other hand, requires a continuous power supply as it is always on and listens for Source queries and Tag responses. Additionally, the Reader is computationally more complex than the Source as it receives from multiple channels to process Tags concurrently, making it more expensive than the Source. Therefore, by separating the Source and the Reader and improving the Tag-Reader communication distance, we reduce the number of power-hungry Readers, in turn reducing the overall infrastructure cost. In addition, energy

harvesting limits the Source to Tag distance but not the Tag to Reader distance. Hence, the decoupled system allows strategic coverage of large areas with distributed inexpensive Sources and Tags, while using a single Reader to cover the entire range.

Two main design choices pave way for the battery-less operation of PACT Tags employed with active radio. First, the Tag responses (yes or no) are short and hard-coded on the Tag; since the answer to a Query is either yes or no, Tag response is independent of the length of the sensor data. Therefore, despite the higher power consumption of active radio, its **on-time is much smaller**, resulting in a lower energy consumption than that of backscatter tags. Second, to reduce the on-time of the Tag, we leverage a low-power envelope detector as a **wake-up receiver** that activates the rest of the Tag only when a valid Query is received. This in turn reduces the overall Tag energy consumption. Thus a PACT Tag (with active radio) can operate in real-time using only the energy harvested from an off-the-shelf RF transmitter as the Source and a decoupled receiver as the Reader.* All the circuit diagrams, PCB files, and software to recreate PACT have been made publicly available [76]†.

PACT Source Design: We implement a PACT Source using TI CC1125 [77] as the radio with MSP430 [78] as the microcontroller (MCU) interface. Periodically, the MCU triggers the Source to transmit an ASK modulated Power-up sequence and a Preamble, to wake up the Tag, followed by the question; e.g., "Is the input less than 30?". For outdoor range experiments, the Source EIRP is set to 16 dBm - maximum transmit power of CC1125 is 14 dBm, along with an antenna gain of 2dBi. This is within the FCC limits of 30dBm. The Source operates in the 902 - 928MHz ISM band at a baud rate of 9.6kbps. In section 3.3.1, we present our Query design in detail.

PACT Tag Design: Figure 3.1 summarizes the prototype of a PACT Tag that

*The number of queries and the maximum length of a Query depends on the application; an optimal Query design is part of future work.

†https://github.com/UW-CONNECT/PACT

Table 3.1: Comparison of State-of-the-art ultra lower power communication technologies

Technology	Battery less tag	Comm. range > 10m	Number of concurrent tags>10
Active RFID [79]	✗	✓	✓
WiFi Backscatter [15]	✓	✗	✗
BLE Backscatter [80]	✓	✗	✗
Passive RFID [65]	✓	✓	✗
HitchHike [44]	✓	✓	✗
PLoRa [12]	✓	✓	✗
LoRa Backscatter [9]	✓	✓	✗
LoRea [67]	✓	✓	✗
PACT	✓	✓	✓

includes an energy harvesting module, an FPGA (Digital Comparator) for Preamble and Query matching, and an active radio that responds to the Reader. The Tag includes a half-wave rectifier with a 15-stage Dickson charge pump with Skyworks SMS7630-040LF [81] Schotkky diodes. These diodes have a low forward voltage drop and hence function even at low incident powers. The Tag is able to harvest energy from incident RF power as low as -21.67 dBm. The antennas on the Tag are impedance matched using an LC Ell network and the L and C values are obtained from ADS Smith chart utility. The storage capacitor is 6.8 µF, designed to meet the energy needs of our PCB with the FPGA and the active radio.

The Tag includes a wake-up circuit and digital comparator to check for valid Query. We implement the low-power wake-up circuit using Skyworks SMS7630-040LF [81] diode in the envelope detector and the comparator [82] to decode the received bit. Our digital comparator circuit is designed on Lattice Semiconductor's iCE40LX FPGA chosen for its low power consumption and its easy-to-use development toolchain. The comparator ensures that the wakeup circuit activates the Tag on the reception of a valid Preamble. The output of this comparator triggers the active radio for transmission of Tag's response. We use ON Semiconductor's AX5043 transceivers [83] operating in the 902-928 MHz ISM band using FSK modulation as the radio. AX5043 is chosen for its low current of 7.5mA at 0dBm transmit power and consumes 14.85µJ of energy at an

operating voltage of 1.8V to transmit a 2-byte payload. We discuss this in detail in section 3.3.2.
PACT Reader Design: Our proposed Reader can be implemented using any off-the-shelf RF receiver with ASK and FSK demodulator to receive the Query and the response respectively. However, in order to evaluate multi-channel operation of the proposed MAC protocol, we design an FSK demodulator using USRP B200 that can filter multiple channels, demodulate Tag response in each channel, and thus support multiple Tags simultaneously as shown in Figure 3.1. Our implementation can support 520 unique channels concurrently.

In summary, PACT combines the strength of RF energy harvesting with the benefits of active radio to improve communication range of battery-less Tags. In Table 3.1, we present the energy-range-scale tradeoff of recent ultra-low-power communication. Technologies that support battery-less tags using ambient signals have low range (rows 2-3). While backscattering using dedicated excitation source can improve the range of battery-less tags, they cannot support a large number of tags due to collisions and interference (rows 4-8). Although active RFID can communicate over long range and accommodate large scale, it requires battery to power tags.

3.3 PACT System design

In this section, we present in detail the algorithm and system design of the PACT Source, Tag, and Reader, towards our goal of improving the communication range of the battery-less Tag with an active radio.

3.3.1 Query Design at the Source

PACT Source delivers energy to the Tag as well as assist in data encoding by querying the Tag with a specific Question. The proposed Query format consists of three segments as shown in Figure 3.2 (b). The first segment is a

Power-up Sequence; a train of bit 1s that provides sufficient energy to power the Tag which then demodulates the Query to respond. In order for the Source to be energy-efficient with a low-latency Q&A session, we derive the shortest Power-up Sequence required to charge the Tag. The sequence length (in bits) depends on the baud rate (R bps) of the Source and the time to charge the Tag to the desired voltage. For a known charging time, t_c, to charge to the desired voltage, V_D, the optimum length of power-up sequence is,

$$\texttt{Power-up sequence length (bits)} = t_c * R. \tag{3.1}$$

We design and optimize an energy harvesting unit to reduce t_c and decrease the Power-up Sequence length.

The next segment is a *Preamble* that is used by the Tag to verify the validity of the query; it also serves as the Tag address. If each Tag has a unique Preamble, its length is at least $\log_2(\text{Number of Tags})$. Such long Preambles are not desirable as it requires long digital comparators at the Tag. Additionally, querying each Tag sequentially will increase the network latency. To overcome this, we propose a MAC protocol, discussed in detail in section 4.4.4, to query and receive from hundreds of Tags concurrently and reduce network latency. The last segment of a Query is the Question itself. We leverage the prior knowledge about the sensor at the Tag to ask questions of the format "Is sensor data below X?" by sending **X** whose length exactly matches the resolution of the Tag data.

In other words, the Tag is designed to receive **X** and proceed to answer "Is sensor data below X?" by comparing **X** to its sensor data. In order to determine if the sensor data is below X, we introduce *Control bits*, which serve as a mask for each bit of the Question. For example, the Source can ask the Tag if the data is less than 128 by sending an 8-bit Question with the Most Significant Bit (MSB) set to "0". A successful comparison of MSB is sufficient to conclude if the sensed data is less than 128. All the other

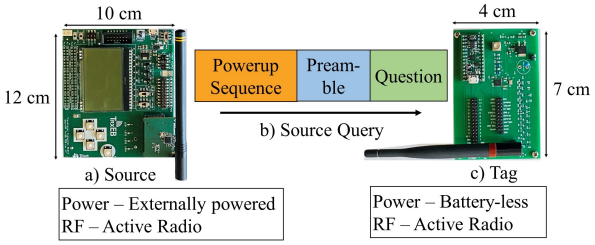


Fig. 3.2: (a) Externally powered PACT Source transmits a (b)Query that consists of a power-up sequence to charge the battery-less Tag, Preamble to check for Query validity, and Question to be compared with the sensor data. (c) Battery-less Tag responds with an active radio.

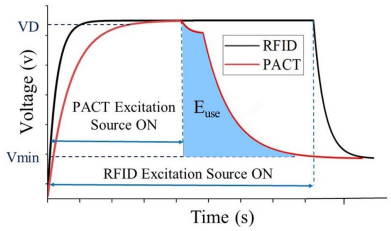


Fig. 3.3: PACT vs RFID capacitor charge-discharge pattern. Backscatter excitation source is ON throughout the operation. PACT Source is ON only till the capacitor charges to V_{max}.

bits are masked by enabling the control bit corresponding to the MSB and disabling comparison of all other bits. More details on control bits are presented in section 3.3.2. The proposed Query format with control bits offers flexibility in the resolution of the data being queried with an optional choice of all 1s as control bits to know the exact match.

3.3.2 Tag Design

The Tag is activated by harvesting energy from the Query following which it demodulates and receives the Question, compares it with the sensor data and responds accordingly using an active radio. Since the query reception and the active radio are powered by the harvested energy, it is crucial that the Tag design is extremely energy efficient. In this section, we present our design of each component in the Tag block presented in Fig. 3.1.

Energy Harvesting Unit:

The harvesting circuit of the Tag includes a half-wave Schottky diode-based rectifier to convert the incident RF energy to DC voltage. It is then

amplified by the following stages of Dickson charge pump. Schottky diodes with low forward-bias voltage enable the Tag to operate at low incident powers [84, 85].

The energy harvesting unit of PACT differs from backscatter systems in one key aspect: backscatter tags harvest energy throughout their operation, while PACT Tags harvest energy for a predefined duration and then use it to operate the Tag. In other words, the incident RF power at the backscatter tag must be above a threshold such that the storage capacitor can be charged in real-time. At distances over 15m, although it is possible to harvest the necessary energy, the time to harvest increases due to the reduced harvesting efficiency at lower incident power. Based on our experiments, this increase in harvesting time affects real-time operation. On the other hand, a PACT Tag first harvests energy from the power-up sequence and then turns the rest of the Tag ON to process. At higher distances with lower incident power, it can still harvest sufficient energy from a longer power-up sequence. Therefore, by designing the power-up sequence to match the charging time of the capacitor, we improve the harvesting range of PACT.

This decoupling of energy harvesting and Tag operation changes the demands on the storage capacitor of a PACT Tag. We illustrate the charging and discharging pattern of an backscatter tag and PACT Tag in Fig. 3.3. We note that a backscatter tag need not store energy, as the excitation source is on throughout the operation. Hence, a small capacitor that can charge/discharge quickly is preferred for backscatter tags. The PACT Tag , however, has two unique requirements: - **the time taken to charge** must be **small** to optimize the power-up sequence length and **the total energy stored** in the capacitor must be **high** to operate the active radio. However, these are conflicting needs, as the total energy stored and the time to charge have a conflicting relationship to the size of the capacitor: smaller capacitors charge faster but store less energy.

Additionally, the voltage across the storage capacitor must be at least V_{min}, the minimum voltage required to operate the Tag components, including the active radio. We design the energy harvesting circuit to meet the energy and voltage needs of the Tag. To enable faster charging, we optimize for the storage capacitor to be the smallest capacitance that can charge to the desired voltage, $V_D > V_{min}$ AND store enough energy to ensure error-free Tag operation. Charging to a higher than required voltage ensures that the Tag will have responded by the time the capacitor discharges to V_{min}. We refer to the total energy supplied by the capacitor in discharging from V_D to V_{min} as the *usable energy* as shown in Fig. 3.3. The energy consumption of the Tag, E_{tag}, must be less than the *usable energy*, E_{use}, given by:

$$E_{tag} < E_{use}, \quad \text{where, } E_{use} = \frac{CV_D^2}{2} - \frac{CV_{min}^2}{2} \tag{3.2}$$

We first determine the capacitor satisfying this inequality. Then, we increase the number of amplification stages from 4 (typical in backscatter [84, 17]) to 15 to generate the adequate voltage for operation, V_{min}, while keeping charging time low [84]. This optimization improves the harvesting range by allowing our storage capacitor of 6.8µF to charge to the desired voltage even at low incident powers. While an RFID tag requires atleast -15dBm incident power, a PACT Tag can charge from -21.67dBm incident power by harvesting for a longer duration.

µW Power Wake-up Receiver and Demodulator

On harvesting sufficient energy, the Tag must start receiving samples. Since our Tag is battery-less, an ultra-low-power demodulator is required. Following the design principles of other low-power wake-on radios in RFIDs and WISP [17, 34, 35, 86, 37, 87, 88, 36], as shown in Figure 3.1, the next stage of the Tag is an envelope detector. We design the Preamble

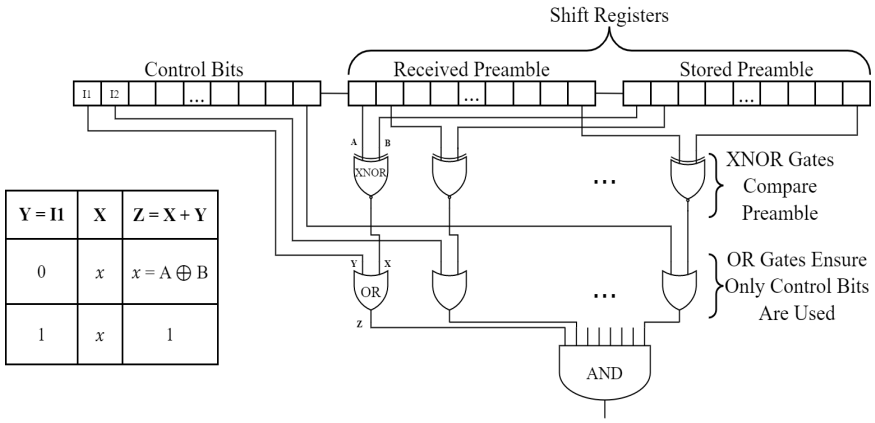


Fig. 3.4: Digital comparator circuit with control bits for Preamble and Question comparison implemented on the FPGA. Control bits mask Preamble/Question bits not to be compared allowing real time changes in the resolution of sensor data.

and the Query transmitted by the Source to be amplitude modulated. On the Tag, a Schottky diode-based envelope detector and an ultra-low power comparator is used to detect, demodulate and digitize the received samples to bit0 or bit1. To do so, a voltage divider holds a threshold on the negative input of the comparator to half of the input power that is received on the antenna. This allows the circuit to adapt to various power levels and receive at longer distances. The received bits from the comparator are stored in shift registers and compared with the known Preamble at the Tag to verify the validity of the received query. In order to conserve the harvested energy, the rest of the Tag is ON only upon detecting a valid Preamble.

Digital Comparator to Validate Preamble and Question:

The digitized Preamble bits are compared with the Preamble assigned to the Tag to check its validity. This preamble check should have low false negatives so as not to miss any Query from the Reader and it must also have low false positives to ensure that the Tag is not triggered ON unnecessarily.

We propose a digital comparator that is resilient to fluctuations in incident power while consuming low energy to conserve the harvested energy [89]. The received Preamble is compared **bit-wise** with known, tag-specific preamble using XNOR gates as illustrated in Fig 3.4. Upon a match, the XNOR gate sets the output high (bit "1"). The result of each bit comparison is input to an AND gate. When all the bits match, the output of all the XNOR gates and hence the AND gate is high. Even if one of the Preamble (or Question) comparison fails, the AND gate output is pulled down (bit '0'). Therefore, a bit "1" output of the comparator indicates a valid query, triggering demodulation of the rest of the query.

The Question follows the Preamble in the Query. The above digital comparator for checking preamble validity is reused for bit-wise comparison of the Question segment with the Tag data. For Question comparison/-match, the received question bits replace the Preamble bits and the Tag data replaces the stored Preamble in Figure 3.4. A Source Query is of the format "Is sensor data below X?" In order to perform this greater than or less than comparison, we propose a modified comparator circuit with control bits.

We design the Source to send a set of control bits for each corresponding Preamble (and question) bit. For example, in order to ask a 16-bit question or preamble, a Source would send 16 control bits ahead of the question or preamble. The **control bits are active low** i.e., a control bit '0' indicates that the corresponding question bit must be compared. A control bit set to '1' implies that the corresponding question or preamble bit is not to be compared. The output of the XNOR gates that indicate whether there was a match, along with the control bits, is fed to the OR gate. When the control bit is set (bit value of '0'), the output of the OR gate is equal to that of the XNOR gate. This means that the OR gate outputs '1' if the corresponding bits match and '0' when there isn't a match. When the control bit is not set (bit value of '1'), the output of the OR gate is always

'1'.

Consider the truth table in Fig 3.4. Y is the control bit and X is the output of the XNOR gate that indicates a match (or not). Any time Y, the control bit, is '1', the output is masked to '1', irrespective of the value of X. When the control bit, Y, is '0', the output of the OR gate is the value of X, which is the output of the XNOR gate. The control bits can thus override the output and in doing so, provide bit-wise question flexibility to the Source; the Source can query the Tag on whether the sensor data is below a value by masking appropriate question bits. Irrespective of the XNOR output regarding bit match, the output is masked and is not considered. The addition of a few OR gates doesn't affect energy substantially but provides for immense flexibility and bit-wise granularity to the matching circuit. This digital circuit can be implemented with a small budget of 794 transistors. The proposed Tag with mostly passive components for Query reception and comparison is energy-efficient and we show that it operates only on harvested energy even at distances up to 24 meters.

3.3.3 Tag Response and Reader Design

To improve the communication range of a battery-less PACT Tag, we propose the use of active radio for the response. However, an active radio is power-hungry; most Commercial Off The Shelf (COTS) radios draw between 5 and 50mA current depending on the transmit power. For instance, CC1125 [77] consumes 220mJ of energy to transmit a 16-bit payload (and a 2-byte header) at a baud rate of 9.6kbps. RF harvesting will be insufficient to power the Tag. In this section, we design the response format to be energy-efficient in order for the Tag to be battery-less. To reduce Tag energy ($power \times duration$), we design a short response that renders the radio ON time (and hence energy) low enough to be operated using harvested energy, in turn allowing the Tag to be battery-less. In our prototype, a 16-bit, FSK modulated response is sent at 915MHz at 1.2kbps baud rate

and 0dBm power.

First, we assign a unique bit sequence to transmit *yes* and *no* in response to the question from the Source. On receiving a Query and matching the data, the Tag activates the active radio to send the corresponding response (yes or no). Therefore, irrespective of the Query length and/or the number of queries, the duration of a Tag response is constant, and is equal to the length of *yes* or *no*. Second, we estimate the energy required by the active radio to send a response prior to system setup. Using this estimated energy as E_{tag} in Eqn 3.2, we determine the overall energy consumed by the Tag which will determine the energy harvester configuration. It can be noted that the Tag energy is directly proportional to the duration of the Tag response. If each Tag is assigned a unique bit sequence for yes and no, the response length will increase with the increasing number of Tags. We leverage FDMA (described in detail in section 4.4.4) to maintain short response length. Additionally, with the help of wake-on radio and digital comparator, the active radio remains in sleep/dormant mode until the comparison is complete. We further decrease the energy consumption of the Tag by reducing the transmit power of the active radio to be close to 0 dBm. Due to the simplicity of the active radio, any COTS radio that satisfies the energy budget can be integrated with the proposed Tag. We discuss the Tag implementation and its components in detail in section 3.5.

3.3.4 System Throughput

Due to the question and answer format of PACT, the network throughput characterization is not straightforward. It depends on the number of queries, baud rate of the query, baud rate of response, and the length of the sensor data. While reducing the power-up sequence can improve network throughput by reducing the duration of the Source query, it will lead to lower harvesting range. Therefore, for a given harvesting range, the maximum number of queries that can be broadcast per second by the

Source is determined by the minimum power-up sequence length. We evaluate this relation in detail in section 3.6.1. Network throughput also depends on the baud rate of the response. While higher baud rate allows the Tag to respond faster, the BER (bit error rate) performance of the response suffers at higher baud rates, limiting the communication range. We evaluate the BER performance of Tag responses for different baud rates at increasing communication range in section 3.6.3. Finally, smart Query design can reduce the total number of queries required, in turn improving the network throughput to obtain sensor information with the fewest number of questions. In conclusion, due to the question-answer format, we expect the data rate of a single PACT Tag to be lower than most comparable technologies. However, the overall network throughput can be improved by optimizing the number of queries, modulation characteristics of the Query and response. In the next section, we present our MAC protocol that can accommodate hundreds of PACT Tags to coexist and communicate concurrently to a Reader, further improving the network throughput.

3.4 Scalablity and co-existence of PACT tags

So far, we have focused on a single link with a Source, a Tag, and a Reader. In this section, we focus on the co-existence of multiple Tags in a network with one Source and one Reader, a common topology in practical deployments of applications discussed in Section 3.7. When multiple Tags are within the harvesting range of the Source, more than one Tag could receive the Query and respond. Since the Tags are powered by the Query, the time to harvest, process Preamble and Question, and then respond, is comparable; hence their responses are transmitted concurrently, leading to collisions. A MAC protocol is thus required to uniquely identify each Tag as well as overcome any collisions that may occur as a result of concurrent

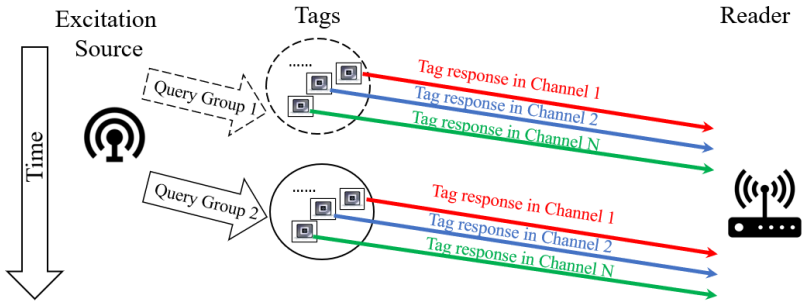


Fig. 3.5: Illustration of PACT's Hybrid MAC protocol : The Source queries a Group, where all the Tags share the same Preamble. The Tags respond concurrently in unique channel which are received by a wide band Reader. The Source proceeds to repeat this for each Group sequentially. Arrow colors in the Tag response indicates a unique frequency channel

responses from the Tags.

One of the widely used anti-collision protocols in RFID is based on Time Division Multiple Access (TDMA), where the Reader interrogates the Tags sequentially [90]. Tag-Driven and Reader-Driven TDMA have also been proposed in backscattering systems [90]. While TDMA-based querying can eliminate collisions, it increases the overall latency. FDMA is not widely used due to the need for oscillators for frequency shift [91]. FDMA also limits the bandwidth (BW) per Tag; lower BW increases the ON-time and energy consumption of the Tag.

We propose a hybrid MAC protocol that is energy efficient at the Tag and the Source; it combines the advantages of TDMA and FDMA to reduce collisions. During system setup, we assign each Tag a unique two-tuple address: (**Preamble, Center Frequency**). The Tags are divided into non-overlapping Groups; each Group has a Preamble i.e., all the Tags within a Group share the same Preamble. Each Tag within a Group is then assigned a unique center frequency (Channel) for the response. When a Source queries with a specific Preamble, all the Tags in the vicinity harvest and perform Preamble comparison. Only those Tags whose received Preamble

match their stored preamble proceeds to demodulate and compare the Question. Depend on the match outcome, the Tags respond a yes or no in their assigned Channel, leveraging FDMA. The Source then continues to Query the next Group with its corresponding Preamble, similar to TDMA. Since each Tag with the same Preamble is assigned a unique frequency, their responses do not collide and are received successfully at the Reader. As the frequencies are reused across Groups, the bandwidth per Tag is higher than that of standalone FDMA. A broadband Reader listening to all the Tags performs FFT to identify all the Tags that replied simultaneously. **Thus, the Source utilizes TDMA to query Groups sequentially and the Tags utilize FDMA to respond concurrently.**

Fig 3.5 illustrates our proposed MAC protocol in a network with one Source, one Reader, and six Tags divided into two Groups. Source first broadcasts a Query with the Preamble set to $Preamble_1$ to query all the Tags in Group 1; Tags can be in arbitrary locations within the harvesting range. After the Query match, Tags in Group 1 reply *yes or no* at their pre-allocated center frequencies, indicated by Channels 1, 2, and 3. The Source then broadcasts the next Query with the Preamble set to $Preamble_2$ to query the Tags in Group 2. Tags in this Group reuse Channels 1 to 3 to respond. Since the two Groups are queried separately, there will be no collisions between Tags across Groups. We optimize the address allocation to maximize the number of Tags without compromising the energy efficiency of each Tag. We propose the following approach to choose the number of channels (and hence Tags) per Group such that the energy consumption of the Tag is minimized. The energy consumption of a Tag (E_{tag}) as shown in Eqn 3.3 depends on the voltage (V_{min}), the current consumption (I), and Δt, the time period for which the Tag is ON. To conserve energy, we choose radio modules that can work at low V_{min}, consume a lower current (I), and/or reduce the "on" time of the radio. For a given radio, V_{min} and I are fixed. Since the ON time of the Tag's

active radio is inversely proportional to its BW of operation (as baud rate is directly proportional to the BW) [92], a higher baud rate has lower ON time and hence lower energy consumption.

$$E_{tag-radio} = V_{min} * I * \Delta t;\ \Delta t \propto \frac{1}{BW};\ \texttt{BaudRate} \propto BW \tag{3.3}$$

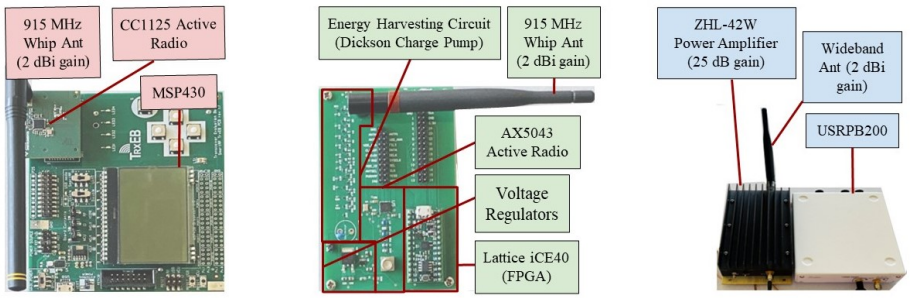
We first determine the energy budget of the Tag radio, $E_{tag-radio}$ to be the difference between the tag energy (except radio) and harvested energy. By substituting the voltage and current drawn by the active radio in Eqn 3.3, we determine the acceptable response duration Δt. The maximum number of Channels that can be assigned with a baud rate such that the response duration per Tag is $\leqslant \Delta t$ determines the number of Tags per Group. The number of Groups is then the ratio of the total number of Tags to the number of unique frequencies. Such a design allows co-existence of multiple tags while maintaining the energy efficiency and range of a single link. We evaluate the tradeoff between the number of frequencies, latency, and energy consumption in section 3.6.5.

3.5 Implementation

We implement the PACT system shown in Figure 3.1 using COTS components and verify the end-to-end performance through simulations and real-world experiments. The prototype used in our experiments is shown in Figure 3.6. All the software, PCB files, and circuit diagrams to recreate the prototype have been made publicly available [76].

Source Implementation:

PACT Source is prototyped using an MSP430 [78] connected to CC1125 [77] radio. The MCU maintains the radio in ASK transmit mode and transmits a Query consisting of the power-up sequence, Preamble, and Question.



a) Source b) Tag c) Reader

Fig. 3.6: (a) Source implemented on CC1125 with 2dBi whip antenna (b) PCB prototype of battery-less PACT Tag: RF front end with 2dBi whip antenna is impedance matched. Harvesting unit stores energy on the 6.8µF capacitor, which supplies power to the wake-up receiver, Lattice iCE40 TinyFPGA, and the AX5043 active radio. AX5043 transmits a 2-byte FSK modulated response at 0dBm and 15 kHz BW. (c) USRP B200 with ZHL-42W power amplifier and 2dBi gain whip antenna as Reader

The power-up sequence is a train of bit 1 whose length is determined by the charging time requirement of the Tags. The Preamble and the Question are 8 bits long; along with 8 control bits each, these are transmitted as a 16 bit value. We use a 2dBi gain, quarter-wave whip antenna and the power level at CC1125 is set to its maximum value of 14dBm, thereby achieving an EIRP of 16dBm, well within the FCC limits. The code used for CC1125 transmitter is located at Source/Software [76].

Reader Implementation:

PACT Reader is implemented on USRP B200 as radio, programmed using GNU Radio. ASK demodulator in the USRP receives the Query transmitted by the Source. FSK demodulator in the USRP receives Tag responses in the 902 - 928 MHz band at a baud rate of 9.6kbps. In experiments that use a single Tag, the USRP receives a signal bandwidth of 200kHz at a sampling rate of 200 ksamples/s. We use a band pass filter aligned to the center frequency of the Tag response with 30 kHz passband and 100dB

stopband attenuation. Demodulation is done using the quadrature demod block set to deviation of 5kHz to match the Tag response. However, in experiments where multiple Tags transmit in different channels, the USRP receives a wide band signal at a bandwidth of 2.4MHz and a sampling rate of 2.4 Msamples/s. Parallel band pass filters aligned to the center frequency filter the received samples and downconvert samples in each channel to 120 ksamples/s, which are demodulated to infer the Tag response in each channel. A wideband whip antenna with less than 1dBi gain is connected to a power amplifier [93] providing 25dB gain to the USRP Reader. The PACT design files are being open sourced at [76]. GNU Radio files and other software for Reader implementation may be found under Reader/Software [76]

Tag Implementation:

Figure 3.6(b) summarizes the prototype of a PACT Tag that harvests energy from the Query to operate. PCB files of the Tag and FPGA code may be accessed under Tag/Hardware and Tag/Software [76].

Energy Harvesting (EH) module:

The first module in the Tag is the EH circuit. Our proposed EH circuit (section 3.3.2) includes a half-wave rectifier with a 15-stage Dickson charge pump. ADS (Advanced Design System) simulations were used to study the impact of the number of stages and storage capacitor. We use the SPICE model of the Skyworks SMS7630-040LF [81] diode for accurate simulations (Figure 3.6(c)) which enabled us to easily modify the number of stages from 4 to 15 and storage capacitors in the range of nF to μF, and choose the optimal capacitor. We choose V_D and V_{min} as 1.8V and 4V to provide sufficient energy at the capacitor whose transient response is shown in Fig. 3.3. The antennas used on the Tag were impedance matched using an LC Ell network; the optimum values of the LC matching circuit,

6.5nH inductor and 1pF capacitor, are obtained using Keysight ADS' Smart Component functionality[‡].

The choice of $C_{storage}$ depends on the total Tag energy and V_{min}. The total energy largely depends on the active radio. For our choice of active radio (described later in this section), V_{min} is 1.8V. TI TPS7B88 and ON Semiconductor NCP718 Low-dropout (LDO) voltage regulators are used for 3.3V and 1.8V supplies to the FPGA and radio respectively and require 300mV as the minimum input. ADS simulations indicated that the smallest capacitor needed for a Tag with AX5043 is 6.8μF; hence, we use that in our hardware implementation.

Wake-up and digital comparator circuit:

Following the EH block, the Tag checks for valid Preamble and Query. We implement the low-power wake-up circuit using Skyworks SMS7630-040LF [81] diode in the envelope detector and an ultra-low power comparator[82] to decode the received bit. The comparator operates without any feedback and the output is pulled up to VDD or down to 0 depending on the result of the comparison. Our prototype of the digital comparator is designed on the TinyFPGA BX using Lattice Semiconductor's iCE40LX FPGA [89]. We chose the iCE40LX for its low power and its easy-to-use development toolchain. The digital matching circuit ensures that the wakeup circuit activates the Tag if and only if a valid Preamble is received.

Active radio on the Tag:

We use ON Semiconductor's AX5043 transceivers [83] for the active radio; it operates in the 902-928 MHz ISM band using 2-FSK. We use AX5043 for its low current of 7.5mA at 0 dBm transmit power, consuming 14.85μJ of

[‡]To optimize the impedance matching circuit below -15 dBm power, a variable capacitor is needed to account for manufacturing tolerances of capacitors affecting the precise matching required for optimal harvesting efficiency.

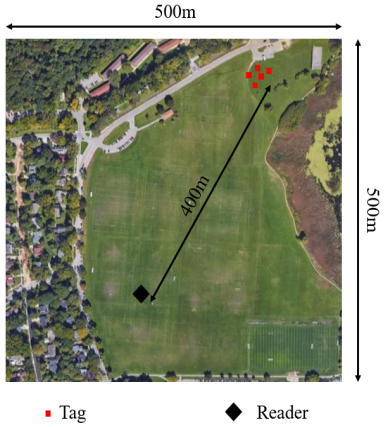


Fig. 3.7: Experimental outdoor set up in a 500 m x 500 m open field to evaluate communication range.

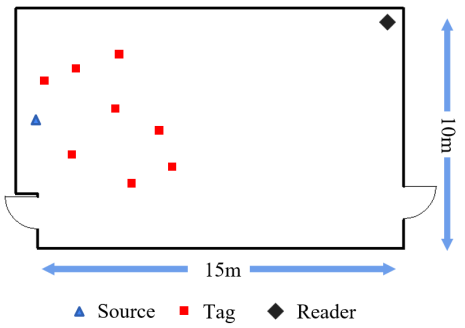


Fig. 3.8: Indoor Setup in a 15m x 10m lab space with up to 8 Tags distributed within 24 meters from the Source

energy. The response consists of an 8 bit header (alternating 0s and 1s) followed by an 8-bit response (yes or no) to the Query. Upon a match, a *yes* response is transmitted by all bit-1 s and a *no* response is transmitted by all bit-0 s. Upon receiving and successfully matching the Preamble, the FPGA turns the radio ON and transmits the 16-bit response. In outdoor experiments where multiple Tags transmit concurrently, we use MSP430 to emulate the FPGA. In these experiments, the MSP was externally powered through a battery and did not use harvested energy. The 2-FSK modulated Tag response is transmitted at a baud rate of 9.6 kbps and 0dBm power. Multiple Sources associated with various Tag groups can be placed up to 400m from a single Reader. In our experiments, we test the worst case by placing the Source and the Tags 400m from the Reader.

3.6 Evaluation

We use the hardware prototype described above and evaluate the functionality and correctness of our proposed communication system. We evaluate and present our experimental results on the following metrics:

1. Coexistence and Communication Range : We evaluate the maximum achievable communication range between a PACT Tag and a Reader, when the Tag is within 24 meters from the excitation Source (maximum harvesting range). We also study the coexistence of 5 Tags in this experiment.

2. Harvesting Range and Communication Range : We characterize our EH unit at various harvesting distances from the Source and evaluate the relation between harvesting and communication ranges. We experimentally evaluate the sensitivity of the Tag at decreasing incident powers.

3. Throughput and RF Energy Harvesting Range : We evaluate the maximum number of queries that can be transmitted by the Source to a battery-less Tag, which determines the per-node throughput. We experimentally show the dependence between throughput and storage capacitor on the Tag. We also evaluate the impact of achievable response throughput at increasing distance between Tag and Reader.

4. Energy Consumption: We evaluate the energy consumed by a PACT Tag and Source to convey a 2-byte payload and compare it against state-of-the-art backscatter systems and Active RFID.

5. Network Latency : We evaluate the network latency for increasing number of Tags and compare against state-of-the-art battery-less tag networks.

Experimental Setup :

Our experiments were conducted in Line-of-Sight (LOS) conditions in indoor lab space as well as outdoor environment for long-range evaluations. In Figs. 3.7 and 3.8, we mark the locations of the Source, Tags, and the Reader in outdoor and indoor settings respectively. Outdoor experiments were conducted in a large open field of size 500mx500m under LOS conditions. As discussed in section 3.5, in the outdoor settings, the Tags are battery powered and do not harvest energy. Hence, no Source was deployed in Fig. 3.7. Active radios in the Tag are set to transmit at 0dBm, to emulate Tag functionality when battery-less. At each distance, over 1000 rounds of query-response pairs were recorded from the Tags on the USRP over a period of 2 hours. The Tags and the Reader were both elevated from the ground by 1m. Indoor experiments were conducted in 15mx10m labspace. The Tags were placed in random locations around the Source. We used up to 8 Tags, each using an AX5043 radio to transmit its FSK response with 15kHz bandwidth at a unique center frequency with a transmit power of 0dBm.

Baselines compared :

We compare the performance of PACT against state-of-the-art Passive RFID tag (SMARTRAC Sensor DogBone [65]), active RFID tag (TAGSENSE-ZT-ZR [79]), pLoRa [12], HitchHike [44], and LoRea [67]. The RFID tags chosen above are commercially available and are considered ultra-low-power for passive and active RFIDs. Although Gen2 passive tags from SkyRFID [21] operate up to 16m range, they do so at the highest EIRP. However, they are not commercially available as yet. Passive backscatter systems with long communication range are chosen as baselines. pLoRa, xSHIFT, and HitchHike use a three-node communication model by incorporating a dedicated excitation source, similar to PACT. LoRea uses a two-node communication model by relying on ambient signals to backscatter data.

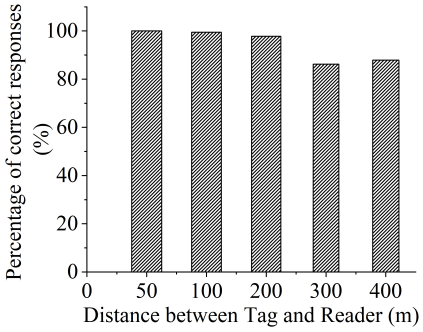


Fig. 3.9: Concurrent responses received from 5 Tags at the Reader. Each Tag responds in a unique channel, with 15 kHz bandwidth and 1.2kbps baud-rate.

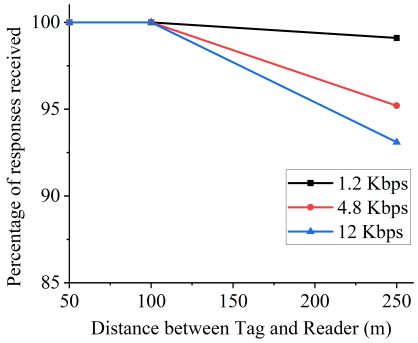


Fig. 3.10: Responses received by the Reader at increasing distances for three different FSK baud-rates used by the PACT Tag for transmitting its response.

To provide a fair comparison, we consider the maximum range reported for pLoRa and Hitchhike and use the corresponding bit rate for energy calculations. We compare against the 2.4GHz implementation of LoRea because it relies on ambient RF signals from WiFi routers as excitation. We recreated Hitchhike tag using the publicly available code-base [94]. For other works, we utilize the power consumption and communication range results as reported in the respective papers.

3.6.1 Coexistence and Communication Range

We evaluate the achievable communication range of 5 PACT Tags, each sending its response at a baud rate of 1.2kbps. Tags were deployed in an outdoor field with LOS to the Reader. In Fig. 3.9, we plot the average rate of correct responses across all Tags as a function of communication range in the x-axis.

We observe that the Reader decodes 100% of the responses from the Tags at 50 meter and over 99.7% of the responses at 100 meters. As the

distance increases, the SNR decreases, in turn reducing the percentage of responses decoded correctly. At a distance of 400 meters, the average rate of correct responses across all 5 Tags is about 88%. It must be noted that the transmit power of the AX5043 active radio is set to 0dBm. Despite this low power, PACT Tags are capable of communicating to the Reader that is about 400 meters away. This is due to the use of ultra-narrow bandwidth of 15kHz, which decreases noise floor and improves SNR. In addition to improved range, ultra-narrowband operation improved scalability by increasing the number of available channels. The achievable communication range of PACT also depends on the baud rate of the Tag response, as shown in Fig. 3.10. As the baud rate of the response increases, the success rate decreases beyond 100 m. The communication range-throughput tradeoff is discussed further in section 3.6.3.

Due to the high cost of the FPGA (over $200), we prototype only one Tag with the FPGA. However, an FPGA is closer to chip design than an MCU so despite the FPGA prototype being expensive, a chip form factor at scale (much like RFID tags) will bring down the cost of each Tag. To evaluate the co-existence of Tags, we implement PACT Tags on MSP430 with AX5043 as the radio. In this setup, we only evaluate the Tag to Reader communication range, and do not implement the energy harvesting component of the Tag. We independently verify that at the maximum energy harvesting range of 24 meters, the Tag harvests sufficient energy to operate AX5043 radio at a transmit power of 0 dBm. Therefore, to emulate networks with maximum harvesting range, the Tag radio transmits at 0 dBm, while the MSP430 is powered using the laptop.

In summary, use of active radios with ultra narrowband operation improves the communication range by enhancing the SNR at the Reader. Additionally, it allows multiple Tags to transmit concurrently in the 902-928 MHz ISM band without interfering with each other and hence allowing PACT networks to scale. We note that the active radio decouples the

Table 3.2: Communication Range (Tag to Reader distance) at increasing Harvesting Ranges (Source to Tag distance) and the received signal strength (RSS) at the Reader.

Technology	Communication Range : Tag- Reader Distance (m)				Max. Harvesting Range (m) (Theoretical)	Max. Harvesting Range (m) (Experimental)	RSS at Reader (dBm)
	Source to Tag $\leqslant$ 1m	1m < Source to Tag $\leqslant$ 5m	5m < Source to Tag $\leqslant$ 10m	10m < Source to Tag $\leqslant$ 20m			
PACT	400	400	400	400	24	24	-31.6
LoRea [67]	225	160	140	90	22*	-	-44.4
pLoRa [12]	600	200	150	-	10*	-	-61.2
HitchHike [44]	54	20	8	-	6*	-	-67
Passive RFID [79]	10	10	10	-	10	10	-32
Active RFID [65]	300	300	300	300	5*	-	-46

communication range from the harvesting range. In other words, a communication range of 400 meters is feasible even at the highest harvesting range of 24 meters.

3.6.2 Harvesting and Communication Range

The use of a separate excitation source to improve communication range has been proposed by other works such as Hitchhike [44], LoRea [67], pLoRa [12]. In existing architectures, the communication range is improved by bringing tags closer to the Source (decreasing the harvesting range). Here, we compare the communication range at different harvesting ranges of PACT and other battery-less, long range communication systems.

Table 3.2 compares the communication range between the Tag and Reader of PACT with other backscatter systems and RFIDs at various harvesting ranges (between Source and Tag). The communication range of PACT does not vary with harvesting range; it only depends on the transmit power of the active radio on the Tag. At a Tag transmit power of 0 dBm, PACT communicates to distances of about 400m (also showcased in Fig. 3.9). This impressive communication range is attributed to the use of

*Harvesting range estimated from the tag power consumption to transmit a 2 byte payload.

ultra narrowband active radio, which faces only one-way path loss. PACT achieves 7× improvement over HitchHike and 40× over Passive RFID tags at a Tag-to-Source distance of 1m for PACT and Passive RFID and 0.2m for HitchHike. 3-node backscatter systems such as HitchHike enhance communication range by compromising the harvesting range i.e.,keeping the excitation source closer to the tag. pLoRa and LoRea have the distinct advantage of using chirp spread spectrum(CSS), which inherently offers greater sensitivity on the Reader, improving communication range up to 225m (LoRea) and 600m (pLoRa). However, to reach these long ranges, pLoRa requires the excitation source to be 20cm away; when the excitation source is 5m away, the communication range drops to around 200m. We observe that a PACT Tag can be adapted to implement CSS to further improve range. Except at harvesting ranges below 1m, PACT Tags achieve the highest communication range (highlighted cells in Table 3.2).

Column 6 shows the maximum harvesting range estimated using the Friis free space propagation model to account for path loss. We achieve an impressive harvesting range of 24m, over 2× improvement over passive RFID. We experimentally verify that PACT Tags require a minimum estimated incident power of -21.67 dBm to charge its storage capacitor over 300mV. The voltage regulators on the Tag can then provide 1.8V to all the Tag components as long as a minimum of 300mV is supplied to the regulators. Assuming the maximum Source EIRP as stated by FCC regulations (30dBm output power through a 6dBi antenna) and minimum incident power of -21.67dBm, we estimate the maximum range possible by using the Friis free space propagation model to be 24m. The improved harvesting range is made possible by the low Tag energy consumption (evaluated in the next subsection) of about 23µJ. Unlike backscatter, which requires the presence of a continuous excitation source for energy harvesting as well as communication, PACT Tags only harvest energy from the Power-up sequence and expend it in a fraction of the charging time

to operate the Tag. For the other technologies compared, we estimate the harvesting range based on their tag energy, minimum operational distance from the Source, and Frii's path loss model. It must be noted that these experiments to determine the sensitivity of the Tag do not include MSP430 on the Tag. We use PACT Tag implemented on the FPGA to perform these experiments.

In summary, PACT decouples the communication and harvesting range by using an active radio. The improvement in communication range can also be observed by the RSS (received signal strength) of various technologies when the Source and the Reader are 1m from the Tag. We assume the maximum Source power as stated in the respective papers. On an average, the RSS at the PACT Reader is 25dB higher. pLoRa uses ambient RF signals to backscatter which results in a low RSS. HitchHike and LoRea use a dedicated Source but the RSS on the Reader suffers due to two way path loss. Even though the RSS of passive tags is comparable to PACT, the SNR is still significantly lower due to self interference by the excitation signal. By incorporating a low power radio on the Tag, PACT is able to increase the RSS, and hence the SNR at the Reader. This allows us to use any COTS transceiver as the Reader without additional components for interference cancellation, making PACT a low-cost solution.

3.6.3 Query Throughput and Harvesting Range

In a PACT network, the overall network throughput depends on the number of query-responses per unit time, baud rate of the Query and the Tag response. In this section, we evaluate the impact of each of these individually.

In Fig. 3.11, we plot the maximum number of queries that can be sent by a Source in a second at increasing distances between the Source and the Tag (harvesting range). As the Tag moves away from the Source, the harvesting efficiency deteriorates and requires longer duration to charge

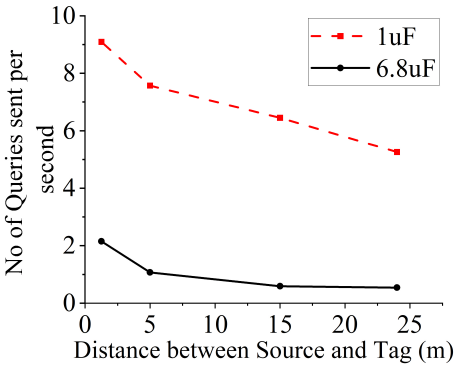


Fig. 3.11: Maximum # of queries that can broadcast by the Source and processed by the Tags Vs harvesting range

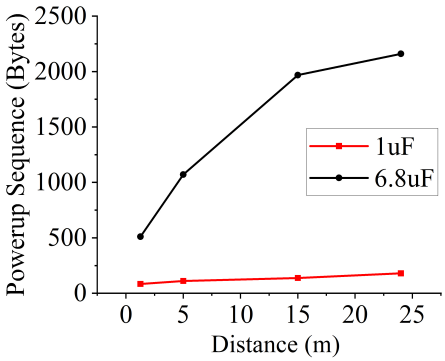


Fig. 3.12: Minimum Power-up Sequence to charge a PACT Tag with AX5043 for two capacitors : 1µF and 6.8µF.

the storage capacitor. Therefore, the Source has to supply a longer power-up sequence to meet the Tag's energy demands. This in turn increases the duration of the Query and decreases the number of Queries per second.

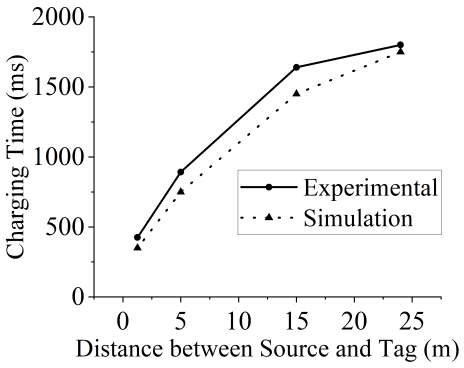


Fig. 3.13: Experimental and simulated verification of the time to harvest and charge Tag with 6.8µF capacitor.

The increase in estimated power-up sequence length (bytes) at increasing harvesting ranges is shown in Fig. 3.12. Additionally, the power-up sequence length varies with the storage capacitor as the charging time depends on the capacitance. As shown in Fig. 3.12, a smaller capacitor (1µF) has a lower impact than a larger one. PACT Tags with lower power active radios will use smaller capacitors and can operate with power-up sequences of few 10s of bytes.

We evaluate the charging time of a 6.8μF capacitor experimentally and through ADS simulations in Fig. 3.13. In our experimental evaluation, we vary the transmit power of CC1125 radio to emulate varying distances. On an average, the experimental charging time is within 87% of the simulation. Since the LC matching circuit in our implementation has been designed for best-case matching at low incident power conditions (i.e., larger Tag-Source distance), our simulation results for larger Tag-Source distances match the experimental evaluation more accurately compared to smaller distances.

We thus show that the Tag energy, storage capacitor, and the expected harvesting range determines the power-up sequence length and hence the number of queries per second. PACT Tag using a 6.8μF capacitor can receive up to 2.15 queries/second when it is 1.2m away from the Source. This number drops to 0.54 queries/second at the maximum harvesting range of 24m away, due to the longer charging time. However, a PACT Tag implemented with a 1μF capacitor can receive 9.09 and 5.26 queries/second at harvesting ranges 1.2m and 24m respectively. While the harvesting range does not affect the communication range of PACT Tags, it affects the network throughput. The longer the distance between the Source and the Tag, lower is the per-node throughput.

The second factor that impacts the throughput is the baud rate of the Tag response. We plot the percentage of Tag responses that were decoded accurately by the Reader at increasing distances between the Tag and the Reader (communication range); we evaluate the decoding accuracy when the responses are transmitted at baud rates of 1.2kbps, 4.8kbps, and 12kbps in Fig. 3.10. Tag response at a higher baud rate reduces the transmission time and hence improves throughput. However, higher baudrate leads to higher probability of symbol errors. As shown in Fig. 3.10, at distances of 50 and 100m, a PACT Reader demodulates 100% of the responses at all three baud rates. As we move further to 250m, the packet decoding

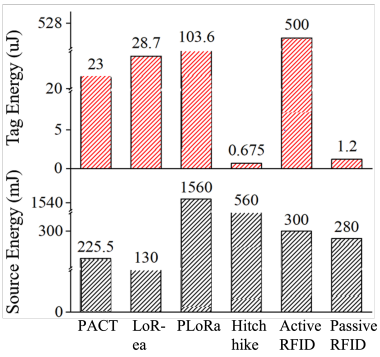


Fig. 3.14: Comparison of the average energy consumed by a Source (bottom) and a Tag (red) transmitting a 2-byte payload by different technologies

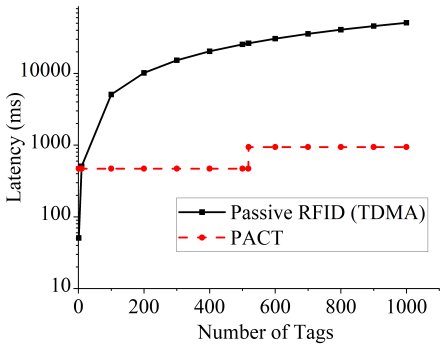


Fig. 3.15: Estimated Network Latency as network size grows : PACT results are based on the experimental setting of Tags using FDMA with 15kHz BW

accuracy drops to 93% for 12 kbps.

In summary, the network throughput of PACT can be improved by increasing the baud rate of Tag response at the cost of reduced communication range. It can also be improved by decreasing the power-up sequence length, which increases the Query throughput by trading off the maximum harvesting range.

3.6.4 Tag and Source Energy Consumption

We evaluate the energy consumption of PACT Tag as low energy consumption is necessary for its battery-less operation. Since the active radio is the most power-hungry module of a PACT Tag, we also analyze the Tag energy when using active radios with lower power than that of AX5043. We identify Langevelde [95] as a potential low-power active radio that draws 1.8mA at 1.2V. We measured the current consumed by our prototype with AX5043 using a 6.5 digit Keysight multimeter and the benchvue tool. Benchvue also lets us verify the ON time of the Tag for energy calculation. We also present the energy consumed by the PACT Source. Unlike

backscatter systems where the excitation source is ON throughout the communication, a PACT Source is ON only for the duration of the Query and then goes back to sleep, thus conserving the Source energy. Reducing the Source energy renders PACT to be a sustainable network with the potential to power the Source from a battery, making PACT more accessible for applications such as transportation tracking, livestock monitoring among many others.

Fig. 3.14 plots the Tag and Source energy for PACT and other passive systems. The energy consumption of a PACT Tag implemented with AX5043 is higher than that of other passive systems. However, when implemented using Langevelde [95], it is 33% and 74.9% lower than pLoRa and LoRea respectively, because the Langevelde radio operates at a 2x lower voltage, and draws over 3x lesser current than AX5043. We recreated and experimentally verified the Tag energy of Hitchhike. For fairness, we compare the PCB implementation of each technology and not ASIC. Majority of existing work focuses on reducing the Tag energy at the cost of increasing the Source energy. On an average, the Source energy of PACT is at least 23% lower than that of various backscatter technologies compared in the Fig. 3.14. LoRea relies on ambient RF to backscatter and hence has low source energy of 130mJ, compared to 225.5mJ consumed by the AX5043 implementation of PACT. However, the Langevelde implementation of PACT reduces the Source energy to 5.5mJ due to reduced power consumption of the radio. It must also be noted that the Source energy in PACT is amortized over all the Tags that transmit concurrently. In our evaluation, even though the overall energy consumed by the Source is 225.5mJ, all 5 tags are charged simultaneously and no additional energy is incurred. Hence, as the system scales up, the energy consumption of the Source remains constant. On the contrary, other backscatter tags that do not transmit simultaneously increases their source energy consumption linearly as the system scales. This is of particular significance in applications where

the Source could be battery powered.

3.6.5 Network Latency

We evaluated the coexistence of 5 PACT Tags experimentally in section 3.6.1 and showed that they communicate with a wide-band USRP Reader placed up to 400 meters away. In this section, we show that over 500 concurrent Tags can operate in a single group with the bandwidth setting in section 3.6.1 in the ISM band. Additionally, the network size can be increased further by adding new Tag groups with minimal impact on network latency.

In our experimental evaluation with 5 Tags, each Tag is assigned a unique center frequency and is programmed to transmit the response using 15 kHz bandwidth 2-FSK response. Nearest adjacent channels were designed to be 50 kHz apart i.e.,the difference between the center frequencies of any two Tags is an integer multiple of 50 kHz. With a bandwidth of 15kHz, this above difference allows a guard band of 35 kHz between two adjacent channels. We validate experimentally that at this guard band, the energy leakage from one channel to the other is little to none. Additionally, with a 100 dB attenuation loss in the Low pass filter at the Reader, a 50 kHz difference between center frequencies ensures no interference from adjacent channels. Given the 26 MHz spectrum between 902MHz and 928MHz, up to 518 channels that are spaced 50kHz apart can be received concurrently by the Reader. Therefore, a Source can broadcast its Query over 500 Tags and the Reader can receive all of them simultaneously in one group. However, the computational complexity of the Reader to receive a 26 MHz wide spectrum and process over 500 low pass filters and demodulators is significantly higher than that of a Reader processing a single Tag. Wide band software defined radios for [96, 97, 98] IoT applications have been a growing research area that we believe offer low-cost design for PACT Reader. Our current implementation using USRPB200 is

limited to 2.4MHz spectrum, due to the limitations of sampling rate that can supported by the computer.

To illustrate the advantage of our hybrid MAC protocol, we compare the network latency of PACT network as a function of number of nodes in Fig. 3.15. We define network latency as the overall time to obtain data from all the Tags in the network. We compare against TDMA, a commonly used MAC protocol by RFID systems. While TDMA is easy to implement and can scale up to 10s or even 100s of devices, in addition to higher Source energy, it has the disadvantage of increasing network latency. The latency of TDMA and our proposed MAC approach for a varying number of Tags is shown in Fig 3.15. PACT's latency remains constant for a group of up to 518 Tags. It increases linearly with the number of groups i.e. the latency increases only when the network size steps up by an additional 518 Tags in this setting. This is in contrast to passive backscatter, where the latency increases linearly with the number of Tags. The advantage of our hybrid MAC protocol is evidenced by the fact that the latency of a network of 500 - 1000 PACT Tags is the same as the latency of a network of 10 passive backscatter tags. Such low network latencies even in a large-scale deployment leads to faster tracking, which in turn improves throughput.

3.6.6 PACT v/s Passive RFID Comparison : A Case Study

Let us consider a warehouse shelf with 100 cartons each containing perishables that could be spoiled below 8 °C. A PACT Tags per carton is placed on the shelf and a Source to Query these Tags is deployed within 24 meters of the shelf. The Reader is located in the corner of the warehouse, listening to the Source and the Tags. The Source asks the Question "Is the temperature less than 8 °C?" and all the Tags respond concurrently on their respective channels. The Reader records all the responses and uploads them to a cloud server. For an RFID deployment, a minimum of 2 RFID readers are required to cover the entire shelf. We assume that the

Table 3.3: Comparison of PACT prototype using COTS components with Passive RFID.

	PACT	RFID
Harvesting Range	24 m	10 m
Communication Range	400 m	10 m
Tag Energy	23μJ	1-2 μJ
Source Power	150 mW	-
Reader Power	700 mW	1 W
Latency	470 ms	5083 ms
Tag cost	$50 - $290	$0.1 - $20
Source cost	$50	-
Reader cost	$1175	$1250 - $2700 [33]

tags don't move and that the reader position is optimized based on the tag locations. The tags transmit the recorded temperature to the reader in a TDMA fashion. All the tags (RFID and PACT) are equipped with a temperature sensor that has an 8-bit resolution.We tabulate the range, energy consumption, communication latency, and cost of all components in Table. 3.3. Passive RFID tags are limited in their communication range due to backscatter based transmission. Only tags that are located within a 10m radius of the reader can communicate with it. To cover larger areas, more readers must be used. PACT decouples the harvesting and communication range; all Tags located within a radius of 400m from the Reader can transmit to it, so long as they are within 24m of the Source. Since all PACT Tags respond concurrently, the overall network latency of the PACT deployment is 470ms. Hence, the Reader and the Source only consume about 400 mJ of energy. On the other hand, due to TDMA based communication, the network latency of an RFID deployment is about 5s which leads to an energy consumption of about 5J. The reduced network latency from concurrent reception at the PACT Reader amortizes the Reader and Source energy consumption over all the Tags, thereby reducing the Reader and Source energy per Tag.

In terms of cost comparison, a bulk of the PACT Tag's cost depends

on the FPGA used which can range from $19 [99] to $260 [100]. Hence, a PACT Tag can cost between $50 and $290. However, this is the price of a Tag prototype implemented using COTS components; we expect the price to reduce considerably when implemented as an ASIC. The Source implemented using CC1125 Radio costs about $50 [77] and the Reader implemented using USRPB200 [101] costs $1175. It must be noted that cheaper software-defined-radios such as RTL-SDR can be used as the Reader which brings the price down to $30 [102]. The total cost of the deployment is $1225, excluding Tags. RFID tags usually range between $0.1 [18] and $20 [103]. Assuming $1250 per reader [32], the total cost comes out to be $2500, excluding tags. Note that PACT measurements are from a COTS prototype. The Tag power and cost will be significantly lower per unit at scale in custom chip form.

3.7 Applications

3.7.1 Smarter Food Safety and Traceability

The FDA's "New Era of Smarter Food Safety" blueprint identifies Technology-based traceability, the ability to track a food product throughout the system from the manufacturing unit, transportation, and distribution, as a key problem to be solved to reduce the spread of food-borne illnesses [56, 52]. The winners of the FDA's low-cost or no-cost to the end-user traceability challenge highlight the interest and need for end-to-end digital record of food products [104]. As has been seen with outbreaks in fresh leafy greens and other foods over the past decade [105], anonymity and lack of traceability in the food systems hinder progress in efforts to identify contaminated foods. PACT fits in this architecture seamlessly by leveraging the simple and flexible query design on a Source and Reader that are implemented using general purpose transceivers that can be modified in real time. Moreover, the same Source and Reader can be used for digital tracing

of different foods with no changes required in the system architecture. In a distribution center, the same Source can query "Is temperature below 40 F?" for food products to be refrigerated and "Is temperature below 0 F?" for those to be frozen [106, 72, 43]. With a simple change in the query, PACT can trace a vast variety of sensor Tags attached to packages. Since the Tags are battery less, its lifetime does not depend on the temperature, unlike BLE tags with limited battery life.

3.7.2 Remote Monitoring for Smart Storage and Transit

Temperature is one of the six factors that affect bacterial growth in food that could result in foodborne illnesses due to Potentially Hazardous Foods. Similarly, temperature monitoring is a crucial part of "cold chain", the supply chain of temperature-sensitive biotechnology and pharmaceutical products [107, 108, 109, 110]. However, the specific temperature requirements depends on the product - food, vaccine, medicine. The World Health Organization estimates that about 50% of vaccines may be wasted gloablly every year due to temperature control, logistics, or shipment related issues[111]. According to UNICEF, $1.5 million worth of vaccines were lost in 5 months often due to difficulty in maintaining the cold chain supply [112]. A flexible query-based temperature monitoring system like PACT will be of great use in monitoring the temperature of each product without changing the infrastructure. The granularity of sensing can be varied by varying the number and specificity of questions. PACT can be integrated into existing data analytics infrastructure with the only requirement of attaching a PACT sensor Tag to the product of interest. It must be noted that although temperature monitoring is key in many applications, PACT can be modified to accommodate other sensors such as humidity without any change in Source and Reader.

3.7.3 Temperature Monitoring for Smart Buildings and Data Centers

Millions of dollars could be saved in energy costs using IoT-based predictive maintenance [113, 114]. However, the cost and infrastructure overheads of battery operated sensor tags and readers limit the wide deployment of temperature sensors [115]. Remote monitoring of buildings, Green House, and Datacenter [116, 117] poses a critical need in the age of green and sustainable engineering. Varying needs for temperature, air pressure, humidity among many other factors impacts the energy demands of these structures. Today's uniform one-size-fits-all solution is energy inefficient. However, IoT based monitoring solutions have not been adopted owing to their limitations on battery life and scalability. Use of scalable, long-range communication using batteryless tags in PACT will enable easier adoption of IoT for remote monitoring and energy efficiency for building and structures.

3.8 Related Work

Commercial BLE: A majority of the current commercial solutions [38, 39, 40, 41, 42, 43] utilize Bluetooth-Low-Energy (BLE) enabled real-time monitoring. However, the short life and bulkiness of batteries needed for BLE poses a challenge, particularly in cold storage units, and is not sustainable at scale.

Passive Backscatter communication: Battery-less communication using backscatter - inspired by passive RFID tags - has been proposed as a viable technology [60, 61, 17, 11, 44, 16] to provide connectivity to low-power sensors. Backscatter tags have a small form-factor and are low cost, making them easily scalable. A backscatter tag offloads communication to a remote source/reader. Variants of backscatter transceivers have been proposed [44, 10, 67, 12, 9, 15] to improve their communication range.

Majority of the existing approaches decouple the excitation source from the reader. We compared PACT with many of the recent works in section 3.6 and showed that we improve the communication range and the number of concurrent battery-less Tags that can be supported in a network.

Backscattering ambient wireless signals: Hitchhike [44] proposes backscattering commodity 80211.b WiFi packets, and conserves the tag energy by removing the oscillator at the tag. However, it increases latency when trying to reduce destructive interference. Also, it requires additional hardware to decode the backscattered packets. FM Backscatter [10] utilizes ambient FM signals that are in the order of -30dBm. However, the RF energy harvesting at such powers is extremely inefficient, making the charging time impractical for wearable sensors or monitoring applications. xSHIFT [11] offloads power hungry demodulation to the reader by modifying the excitation signal. However, its range is still limited by the dual path loss.

Energy harvesting circuit designs : Ambient RF harvesting from cellular and broadcast transmitters has been proposed [118, 63] but it requires the tags to be deployed outdoors and limits the application scope. Moreover, the charging time is in the order of a few seconds and the communication range is limited. MAC algorithms have been proposed to reduce wastage [64] but the practical challenges of designing the framework are not addressed. Battery and power management schemes [62] have been introduced to improve harvesting efficiency but the communication range is limited to a few meters. Finally, studies on energy consumption of sensor nodes [119] aim to create theoretical models which may provide insight to building smart cities. However, these do not address practical deployments or the problems of scalability. Also, efficient RFID tag designs [65] and rectennas (rectifying antennas) [66] have been proposed to maximize the energy harvesting range and efficiency. Low power preamble detection has been proposed in [44, 88, 87, 86, 36, 34, 120, 35, 37, 121] to

reduce tag energy. To increase the range from more than 10s of meters, higher receiver sensitivity is desired on the tags. Advancements in energy harvesting is complementary to PACT and can be integrated to further improve its harvesting range.

ID Modulation in RFID: Alternative means of data modulation like interleaving repetition mechanism [122] and shorted/non-shorted tag states [123] aim to increase the decodability by reducing the error rates. However, they rely on backscatter for communication and not to increase the communication range of the tags.

Spread spectrum to improve range: PLoRa [12], LoRa Backscatter [9], LoRea [67] propose to leverage existing LoRa deployments to enable long-range backscatter and design power-efficient tags by introducing a third node. Existing approaches [25] are unable to solve the near-far problem as they both require the activation signal source to be in close proximity. Despite decoupling the excitation source and the Reader, the excitation signal suffers significant path loss depending on the distance between the excitation source and tag.

Asymmetric Communication protocols: Asymmetric communication protocols have been proposed to leverage the knowledge asymmetry in communication systems [124]. This work is inspired by the theoretical analysis on asymmetric communication that utilizes knowledge asymmetry to address resource asymmetry [124, 125]. To the best of our knowledge, this is the first step towards a practical deployment of asymmetric communication protocols in a wireless network.

4 WICHRONOS: ENERGY EFFICIENT TIME MODULATION FOR LONG RANGE, LARGE SCALE NETWORKS

4.1 Introduction

Wireless data delivery is key to real-time data collection and analysis in the fast-growing areas of smart agriculture [126, 127], livestock monitoring [128], and precision farming [129]. Large-scale soil monitoring networks currently use cellular and satellite networks to collect real-time data over a long period of time [130]. Real-time data collection from in-situ sensors in fields throughout the crop season will provide an understanding of the spatio-temporal dynamics of environmental factors and various chemical and biological processes in the soil, which can, in turn, be used to improve soil health and crop growth. However, due to the high infrastructure costs for solar panels and batteries to enable wireless information retrieval, monitoring sensor networks are deployed only at limited locations and have latencies ranging from one day up to one month [130, 131]. Such monitoring systems typically deploy sensors in large fields and share the following requirements:

Long battery life,

Long-range communication to reduce infrastructure costs,

Scalability and co-existence,

Low cost, with less stringent demands on data rate, latency, and payload size compared to traditional networks. For example, sensors used to measure soil moisture, the chemical and biological properties of soil typically have a resolution of 8-12 bits [132, 133, 134], offering a light payload. Also, the gradual change in the rate of these parameters results in reduced demands for data-rate and latency. However, the monitoring systems are

often deployed in harsh, remote environments on a massive scale and are expected to have battery life in the order of years.

Current energy-efficient protocols such as Zigbee [28], blacktooth Low Energy (BLE) [135], and backscattering [136, 8, 12, 13] consume less than 50mW power during active transmission, allowing for a long battery life. However, their communication range is on the order of 10s of meters, and they require infrastructure support for coverage. On the other hand, approaches for long range such as cellular and satellite networks are expensive and energy consuming, limiting the battery life and scalability of the system. In Table 4.1, we compare the battery-life, communication range, scalability, and achievable data-rate of existing wireless technologies. *Evidently, existing strategies for addressing low-power and long-range do not co-exist efficiently in a large-scale network.* This inefficiency can be explained by the impact of bandwidth (BW) on energy consumption, communication range, and network capacity. In an additive white Gaussian noise channel, the maximum channel data-rate is given by,

$$C = B \log_2 \left(1 + \frac{S}{N_0 B}\right), \tag{4.1}$$

where B is the signal BW in Hz, S is the signal power and N_0 is the noise spectral density [137]. A wideband signal can achieve a high data rate, in-turn reducing the time-on-air (the amount of time a channel is occupied). With reduced time-on-air, the active transmit time of the RF module decreases, in-turn reducing energy consumption. However, the signal-to-noise ratio (SNR), $\frac{S}{N_0 B}$, decreases with an increase in BW, since the noise power increases with BW. At long distances, the received signal power decreases due to path loss; hence a lower BW can decrease noise power and increase the SNR. Therefore, a narrowband (NB) signal is more suitable

Table 4.1: Comparison of current wireless technologies and WiChronos

	Battery Life (>1 yr)	Range (>1 km)	Scalable (>1000)	Data-rate (kbps)
WiFi	X	X	X	<54k
Cellular	X	X	✓	<10k
BLE	✓	X	X	<2k
Zigbee	✓	X	X	<250
Passive RFID [20]	✓	X	X	<40
Active RFID [138]	✓	X	X	<40
AmbientBackscatter [8]	✓	X	X	<1
LoRaBackscatter [13]	✓	✓	X	<37.5
pLoRa [12]	✓	✓	X	<.0002
LoRa	✓	✓	X	<27
SigFox	✓	✓	X	<.6
WiChronos	✓	✓	✓	<1

for propagation over long distances with an acceptable SNR.

$$\texttt{Energy} \propto \texttt{Time-on-air} \propto \frac{1}{B}, \quad \texttt{Range} \propto \frac{1}{B}, \quad \texttt{Scale} \propto B.$$

This conflicting requirement on bandwidth makes it challenging for low-power and long-range solutions to co-exist.

LPWAN (Low Power Wide Area Network) technologies such as LoRa [24], SigFox [26], NB-IoT [27] have been successful in achieving long range [139, 140] and long battery life by limiting the *duty-cycle* (the fraction of time during which a node is in active transmit or receive mode) by reducing the number of messages per day. In other words, existing LPWAN solutions reduce the overall energy by limiting the airtime of each device in a day. They do not address the fundamental tradeoff between low-power and long-range. Therefore, as the network scales, their cumulative airtime will increase, leading to an increase in the probability of collisions, rendering them unsuitable for large-scale deployment.

In this work, we develop a communication framework that addresses the fundamental trade-off between low power and long range in large-scale networks that have relaxed data-rate and latency requirements. *We propose WiChronos, a modulation technique that encodes information in the time interval between two narrowband symbols.* A WiChronos sender transmits exactly two *anchor* symbols per message, namely *preamble* and *postamble*, and the data modulates the duration between them. We leverage the low data rate and small payload requirements of monitoring systems in agriculture, remote tracking, and derive benefits from the availability of resources at the receiver to make transmitters energy efficient.

WiChronos achieves **energy efficiency** by minimizing the number of symbols and (hence the time-on-air) per message, and **long range** by transmitting the anchor symbols over ultra-narrowband (UNB) [141]. The reduced time-on-air and improved spectral efficiency allow the network to **scale better**. WiChronos trades off data-rate to achieve the above three features.

Fig. 4.1 illustrates WiChronos and contrasts it with existing modulations. A WiChronos sender with a sensor data of 678 units transmits an anchor symbol (*preamble*), goes to sleep for 678 clock cycles (that corresponds to data), and wakes up to send another anchor symbol (*postamble*). The anchor symbols consist of a training sequence of alternating 0s and 1s followed by a unique sender address. The sleep time encodes the entire message to be transmitted. The time-on-air of WiChronos is thus independent of the payload length (10 bits in this example) and only a function of the anchor symbols; by separating payload transmission from time-on-air, we reduce the impact of BW on the time-on-air, without affecting the communication range. In the case of traditional modulations such as LoRa or SigFox, the data value of 678 is mapped to bits, which are then mapped to symbols for the corresponding modulation technique and transmitted over the air and hence the time-on-air is proportional to the payload length.

Other time interval based modulations such as M-PPM transmit multiple pulses over air; the time slots in which the pulses are sent indicate the message. In order to achieve a higher datarate, lower latency, and reduce clock skew errors due to imperfect slot synchronization, the number of slots per frame is typically set low. Therefore, the number of pulses is high for longer payloads, in turn increasing the time-on-air.

Towards implementing WiChronos in a wireless network, we identify the challenges in designing an optimal anchor symbol in terms of length, modulation parameters, and medium access control (MAC) in §4.4. We prototype WiChronos using inexpensive off-the-shelf radio modules and microcontroller units (MCU), using software-only changes. Based on our experimental implementation on MSP 430 [142] and Linx-NT [143], we achieved an impressive battery life of over 5 years using a coin cell battery (250mAh) at a range close to 1 km. Also, we estimate the probability of collision to be less than 5% in a 1000 node network under low traffic conditions. To this end, we make the following contributions:

- We propose an energy-efficient modulation technique that encodes information in the time interval between two symbols, minimizing the number of symbols per message.
- We propose a spectrally-efficient physical layer design with UNB anchor symbols, improving the receiver sensitivity and range.
- We implement an ALOHA-based MAC protocol and analyze its robustness to collisions in large-scale deployments, allowing the network to scale seamlessly.
- We prototype the proposed framework using off-the-shelf, low-cost RF modules and MCUs with low-power clocks.

The remainder of this chapter is organized as follows. In 4.2, we provide background on the strategies for low power and long range, and motivate

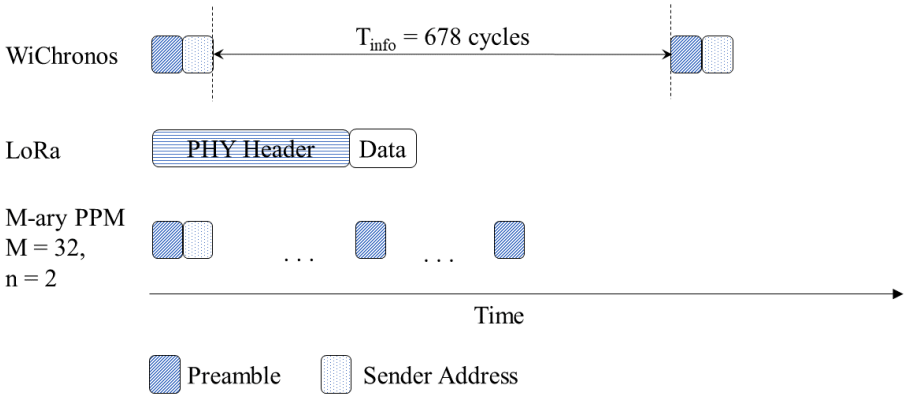


Fig. 4.1: WiChronos illustration

the need for a unifying algorithm in a large-scale network. In §4.4, we present the design and features of WiChronos, followed by a discussion on the challenges and throughput performance in §4.5. Experimental evaluation is presented in §4.6 and some related work is discussed in §4.3.

4.2 Background and Prior Work

The overall power consumed by a sensor node is dominated by the communication module [144, 145]. Algorithms, protocols, and architectures have been developed to reduce the active transmit time and hence reduce the power consumption in the areas of Wireless Sensor Networks (WSN), AdHoc Networks, and Internet-of-Things. We broadly classify existing low power strategies for WSNs into the following five categories [146, 129, 147, 148]:

Duty Cycling,

Routing,

Data reduction,

Radio module optimization,

Energy harvesting and backscatter

Smart sleep/wake-up protocols [149, 150], event-triggered wake-up [151], and scheduled MAC protocols [152, 153] have been proposed to reduce the active transmit and/or receive time of the radio transceiver. Though duty-cycling-based approaches reduce the power consumption of the overall network, they are still limited by the payload length. Data compression [154], prediction [155, 156], and cooperative communication [157, 158] techniques have been proposed to reduce the amount of data to be transmitted, which in turn reduces the energy per message. Network topology-aware strategies have been developed to improve the lifetime of a sensor network through clustering [159], energy-aware routing [160], data gathering, and data forwarding [161]. These approaches decrease the overall energy consumption of the network by leveraging the hierarchical topology and varying the energy constraints of nodes in the network [162, 163]. A new wave of battery-less sensors harvest energy from ambient signals and/or dedicated sources [8, 13] and use backscattering to communicate. However, these techniques are feasible only within a short range and require an additional signal source to piggyback on for long-range communication [12, 13]. Active and passive RFID tags [138, 20] are energy efficient but only work for a short range [19] and/or low traffic. RFIDs also are limited by the energy-range-scale tradeoff presented in 1.

As discussed in 1, the limited range of existing energy-efficient strategies can be attributed to the BW and propagation of radio frequency (RF) signals. The range of an RF signal depends on the link budget that accounts for the gains and the losses.

$$P_{Rx} = P_{Tx} + P_G - P_L, \tag{4.2}$$

where P_{Rx} is the received power, P_{Tx} is the transmit power, P_G is the

antenna gains of the system, and P_L is the aggregate loss due to filter/cable attenuation, known experimental conditions, and path loss (P_{PL}). Free space path loss is given by

$$P_{PL} = -10 \log_{10} \frac{\lambda^2}{(4\pi d)^2} = 22\text{dBm} + 20 \log_{10} \frac{d}{\lambda}, \tag{4.3}$$

where d is the distance between the sender and the receiver, and λ the wavelength. Radio optimization techniques to improve P_{Tx} such as directional antennas [152], Multiple-Input Multiple-Output, and mobility-based solutions such as Mobile Ad-Hoc Networks [164, 165, 166] are energy consuming and not suitable for low-power communication. Given the FCC limit on transmit power, the link budget depends on the path loss, which is inversely proportional to the wavelength (i.e., path loss increases with increasing frequency).

Existing technologies for long-range such as cellular networks, NB-IoT, Sigfox, and LoRa operate in the sub-GHz bands to reduce path loss. Cellular and NB-IoT require high-complexity RF front-end and LTE infrastructure for scheduling and synchronization [167].

SigFox and LoRa operate at lower BW to achieve long range, leading to an increase in the time-on-air. Similarly, Zigbee 3.0 [48] reduces datarate and increases transmit power to improve range inturn increasing time-on-air. To achieve long battery life, LPWAN solutions limit the number of messages per day. Therefore, as the number of messages increases, the overall energy consumption increases, making them inefficient for an energy-constrained system. Also, with increasing scale, collision rate increases, which leads to a decrease in the network throughput [24, 26, 27].

To summarize, existing energy-efficient and long-range strategies cannot co-exist in a large-scale network. In this work, we develop a communication framework for real-time monitoring system that is energy-efficient, communicates over long distances, and supports a large number of nodes.

4.3 Related Work

Timing interval based communication has been studied in the past. We present an overview of these works below.

Information Theoretic Analysis : An information theoretic analysis of encoding information in the queuing time has been studied in literature [168, 169, 170, 171, 172]. While bounds on channel capacity of single-queue and multiple-queue servers worst-case timing error distributions have been studied, they do not provide algorithms for energy efficiency and/or long-range communication in a wireless system. The maximum achievable data-rate of WiChronos aligns with the capacity of timing channel derived in [168].

Timing Channel: Timing based communication has been studied as a security risk in covert timing channels [173, 174, 175], where information is encoded covertly in the time interval. The majority of the research work on timing channels has focused on defense mechanisms to eliminate timing channels.

Pulse Time Modulation: This work is motivated by Pulse Position Modulation (PPM) and Communication through Silence [176], a challenges paper on timing based modulation in wireless sensor networks. [176] does not consider long-range and scalability in wireless networks. It does not consider the challenges in the practical implementation of timing interval modulation in wireless networks such as anchor symbol length, synchronization, and packet errors. To the best of our knowledge, WiChronos is the first attempt at implementing timing interval modulation technique for long-range, energy efficient communication in wireless networks.

PPM and its variants such as Differential PPM [177, 178], M-ary PPM [179, 180, 181, 182, 183] have been developed and widely used in one-to-one optical networks with ultra wide bandwidth and narrow pulses. The following requirements of typical PPM implementations make them challenging for wireless networks.

Bandwidth requirements: PPM and its variants typically use an ultra-wide bandwidth [179] to get a narrow pulse to achieve reasonable data rates while also saving energy. Ultra wide band will result in an increase in energy consumption and noise floor in a wireless module, affecting both battery life and range. To overcome this challenge, we use narrow bandwidth and achieve long range.
Clock Synchronization: In UWB, the pulses are short and therefore symbol synchronization is required for PPM. DPPM, however, overcomes this challenge by encoding in the time difference between pulses [177]. In this work, we relax synchronization requirements with the help of differential modulation and low data-rates. PPM implemented in one-to-one optical links does not require a dedicated MAC protocol. However, in a wireless network, the pulses collide on air and therefore dedicated addressing and MAC protocol is required [184, 185, 186, 187]. Multiple transmitters, therefore, cannot share the channel without incurring packet losses or increasing energy consumption [188, 189]. In this work, we remove the need for MAC by uniquely identifying the transmitter in each pulse.

Despite its energy efficiency, PPM is not popular in wireless owing to the above challenges. We propose WiChronos, a special case of the more general pulse position modulation for wireless communication and design the modulation to cover a long range and accommodate a large scale. In §4.6, we will compare the energy efficiency, range, and scalability of M-PPM with WiChronos.

4.4 Interval Modulation

In the majority of the digital modulation techniques used in wireless networks, data modulates the characteristics of the carrier signal. For e.g., 2-FSK maps bit 0 and bit 1 to two distinct frequencies, transmitting 1 bit per symbol. The total number of symbols per message, therefore,

Table 4.2: Current consumption of individual modules

		Active Current (mA)	Idle Current (mA)	Sleep Current (nA)
MCU	MSP430 [78]	1	0.7	45
	STM32L[190]	0.45	0.3	140
Tx	Linx-NT [143]	42.5	42.5	1
	CC1101 [191]	27.4	27.4	200
Rx	Linx-NT	22.5	22.5	1
	CC1101	15.4	15.4	200

depends on the modulation technique and the message length. Higher-order modulation techniques such as 64-QAM can encode more bits per symbol, but have larger energy per bit, E_b while lower-order modulations such as 2-FSK have lower E_b but an increased number of symbols per message.

A modulation technique that reduces the number of symbols per message without increasing E_b *is required to achieve energy efficiency.* With this insight, we propose WiChronos, a modulation technique that encodes information in the time interval between two anchor symbols. Fig. 4.1 illustrates an example with an integer data 678 from a 10-bit sensor. The transmitter sends a predefined preamble and waits for 678 clock cycles and then a predefined postamble. The receiver, with apriori knowledge of the anchor symbols of each transmitter, identifies the sender from the preamble and triggers the corresponding timer to start (or stop) on the reception of the preamble (or postamble). In the absence of any timing errors and prior knowledge of clock rate, the number of clock cycles counted at the receiver is equal to that at the transmitter.

The total number of symbols transmitted on-air and the energy consumed by the RF module depends only on the length of the anchor symbols and is not affected by the length of the sensor output (10-bits in this example). WiChronos hence satisfies the two requirements identified earlier for energy-efficient modulation i.e.,

Minimum number of symbols,

Non-increasing energy per bit E_b. In the rest of this section, we discuss the challenges in achieving the promise of WiChronos and propose solutions to address them.

4.4.1 Energy Efficiency

A key insight for the energy-efficient design of WiChronos is that the RF module is the bottleneck of a sensor node [145]. Energy consumed by a sensor node is given by $V \cdot I \cdot \delta t$, where V is the voltage, I the average current drawn for a duration δt. For a constant V and given δt, the current drawn, which determines the energy consumption can be classified into six categories as,

1. I_{a-u}: Active - MCU
2. I_{s-u}: Sleep - MCU
3. I_{i-rf}: Idle - RF module
4. I_{s-rf}: Sleep - RF module
5. I_{r-rf}: Active listen - RF module
6. I_{t-rf}: Active transmit - RF module

Table 4.2 enumerates the above currents for selected OTS hardware. The active and sleep currents of MCUs are few mA and μA respectively, as noted in row 2 of Table 4.2. I_{t-rf} depends on the transmit power of the RF module and the protocols implemented in the transceiver. The active currents of RF module are on the order of tens of mA. Therefore, an energy-efficient transmitter must minimize the amount of time spent in active mode. By encoding information in the time interval between symbols, we reduce the active transmit time of the RF module and the MCU. The energy consumption is further reduced by operating the MCU and the RF module in sleep mode during information transfer (clock count).

Fig. 4.2 details our implementation in MSP430 FR2355. On reading analog data from the sensor, the transmitter converts it to a digital value (D), maps to clock cycles T_{info} (with redundancy to correct for timing errors) and sets TimerA to T_{info}. The MCU triggers the RF module to send a preamble and then set the RF to sleep. The MCU itself goes to sleep mode, with TimerA running in the background. After T_{info} cycles, TimerA interrupts the MCU to turn on the RF to send postamble. Since T_{info} is the time *difference* between the symbols, the transmitter and receiver clocks need not be synchronized. It is sufficient to use the same clock rate. Since the RF and MCU modules are in sleep mode during data transmission (T_{info}), the overall energy consumption is unaffected by the message length. The energy consumption of data transmission is,

$$E = V\,(I_{a-u} + I_{t-rf})\,2t_{anchor} + V\,(I_{s-u} + I_{s-rf})\,T_{info} \tag{4.4}$$

where t_{anchor} denotes the duration of anchor symbols. The overall energy consumption is therefore determined by the modulation parameters used to transmit the anchor symbols, the anchor symbol length, and the corresponding current drawn. Optimum anchor symbol length is crucial to achieving the promised energy efficiency.

4.4.2 Anchor Symbol Design

Predefined preambles and sync words are commonly used in communication systems to indicate the start of a packet, as well as assist the receiver with frame (and/or bit) synchronization. The anchor symbols play the same role; indicate the start of a message (to start and stop clock counting) and assist the receiver to identify the sender. Since we specifically focus on networks with relaxed data-rate requirements, the anchor symbols are transmitted at the order of few kilobits per second over narrow BW. At such low data-rates, the time and the number of bits required for the

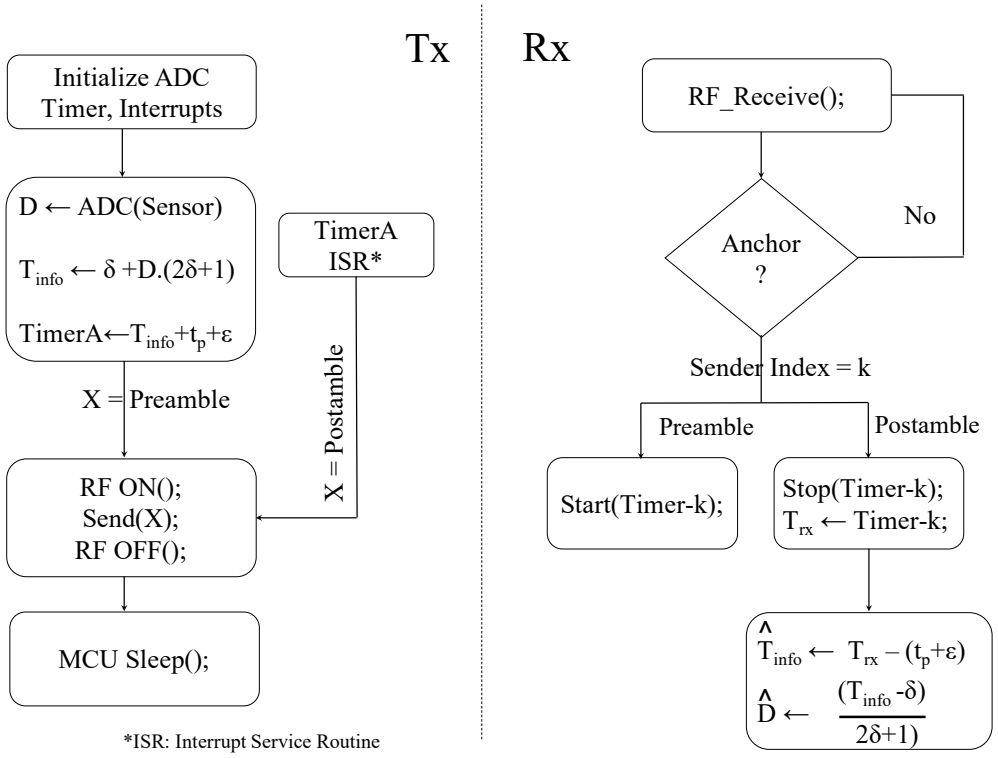


Fig. 4.2: System implementation flow diagram

Automatic Gain Control (AGC) in the RF front end to settle, is reduced. Further, UNB communication requires much shorter preamble than coded modulations [192]. For example, TI CC1125 [77] uses an AGC design with a 4-bit settling time along with smart carrier sensing to reduce false positives. The lower bound on the anchor symbol length is thus determined by the RF front end and the modulation parameters. In order to differentiate between the start counting and stop counting triggers, each sender is assigned two unique addresses i.e., each sender has a unique preamble and postamble.

We define the optimum anchor symbol length to be the shortest length that enables reliable decoding at the receiver i.e., it must minimize the probability of error in decoding and has a low false-positive rate. For a

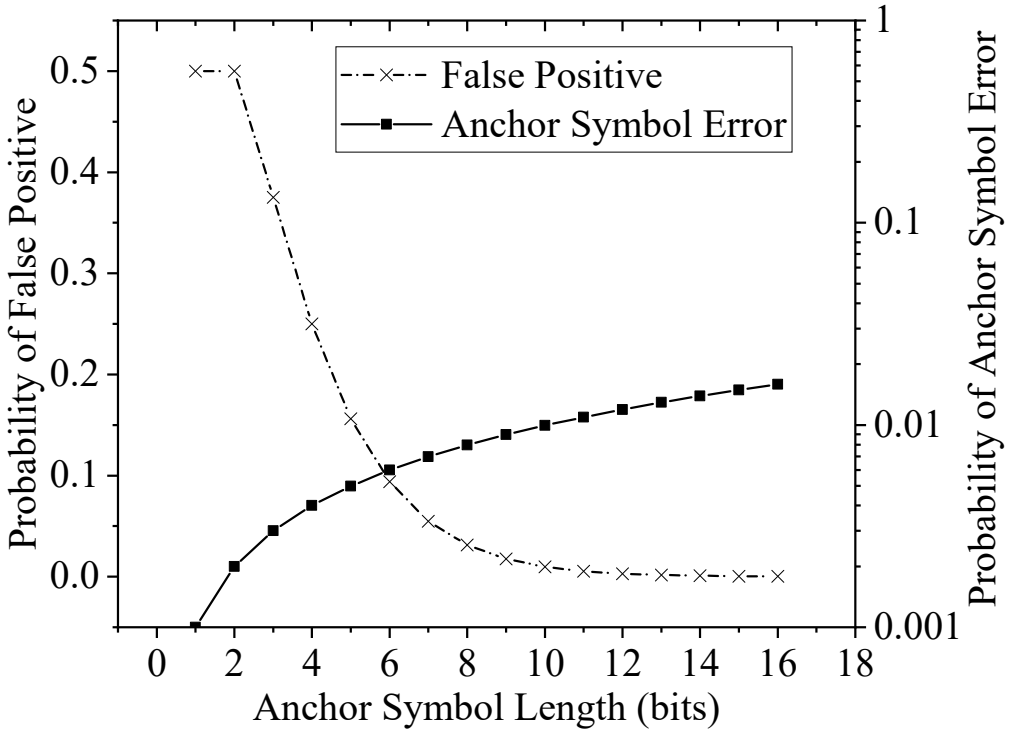


Fig. 4.3: Anchor symbol length design

given modulation, SNR, and the corresponding BER p_b, the probability of symbol error and false-positive are,

$$P_e = \sum_{k=0}^{e} \binom{N}{k} \cdot {p_b}^k q^{N-k}, \quad P_f = (0.5)^N \sum_{i=0}^{\epsilon} \binom{N}{i} \tag{4.5}$$

where e is the maximum number of bit errors that can be tolerated by the receiver for an N-bit anchor symbol. Fig. 4.3 plots the above probability of symbol error P_e and probability of false positive P_f as a function of anchor symbol length for e=0. P_e increases with symbol length; therefore, shorter anchors are desirable to reduce symbol error while P_f decreases with symbol length. With short symbols, the probability of a random bit pattern

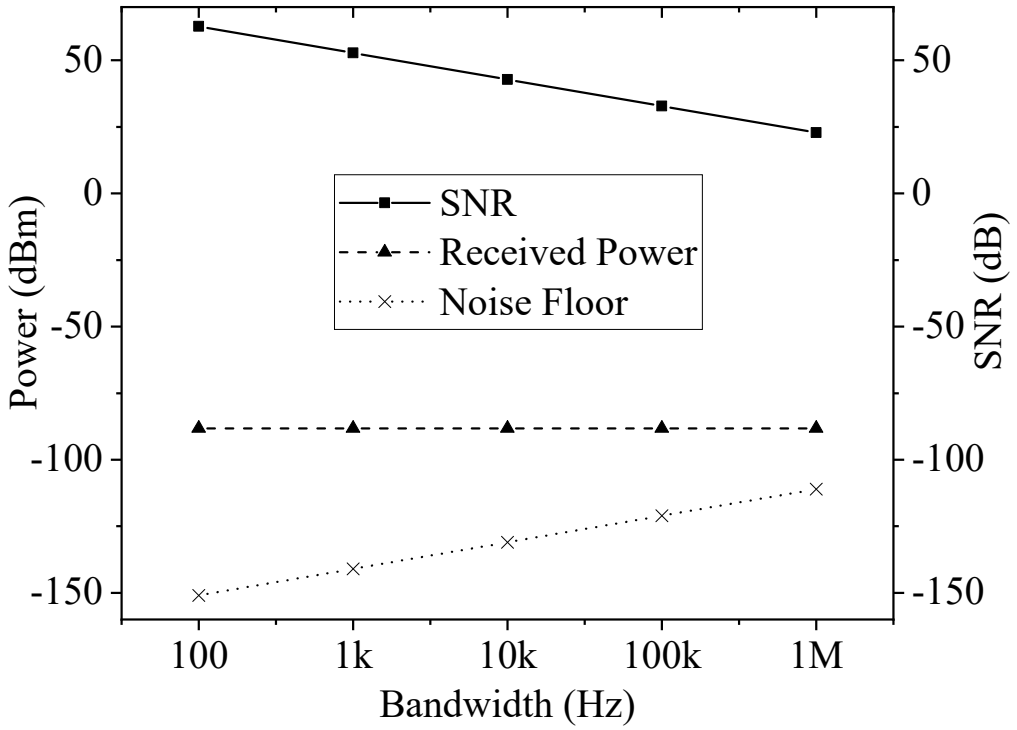


Fig. 4.4: Impact of bandwidth on receiver sensitivity

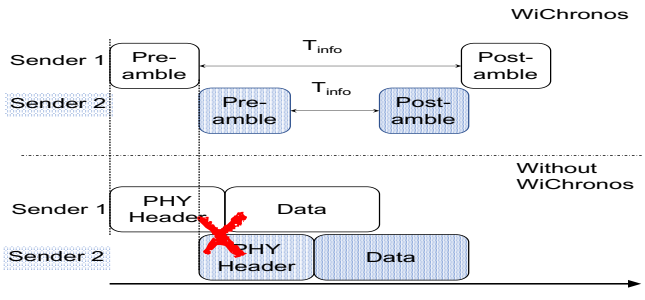


Fig. 4.5: Collisions in the network using ALOHA

from other devices or interference being falsely detected as the anchor is high. We identify the smallest anchor symbol length that renders low P_f and P_e for a given anchor symbol modulation, expected SNR, desired false positive rate, and symbol error rate. In this work, we use BFSK to

modulate the anchor symbols with an SNR $\geqslant$ 10dB, BER of $\leqslant 10^{-3}$. We choose 10-bit anchor symbol to achieve $P_f \leqslant 0.01$ and $P_e \leqslant 0.001$. It must be noted that this shortest anchor symbol length is required to transmit each *pulse* in any variant of PPM. The anchor symbol length calculation is unaffected by the receiver since we leverage the resource asymmetry in infrastructure mode and let the receiver to always be in *listen* mode.

The minimum anchor symbol length is determined by the settling time of the RF module, the probability of false positives, and the probability of symbol error. RF modules with advanced carrier sensing and AGC can further reduce the settling time and false positives, leading to shorter anchor symbols.

4.4.3 Long-Range Communication

The second challenge identified in this work is achieving long-range within the energy constraints. As discussed in 1, propagation loss is directly proportional to the distance and the frequency of operation. Following the IEEE 802.11ah standard [193], we operate in the sub-GHz spectrum and narrow bandwidth (NB) for long-range. The range also depends on the *receiver sensitivity* (the minimum received power required to demodulate the signal with an acceptable BER), a characteristic of the receiver. For a given propagation channel and frequency of operation, the received power from Equation 4.2 depends on the transmit power, antenna gains, and the channel. SNR depends on the received power and the noise floor, given by,

$$\text{Noise floor} = -174 + \mathsf{NF} + 10 \log_{10} \mathsf{BW}. \tag{4.6}$$

Here NF is the noise figure (the ratio of input SNR to output SNR at the receiver) and BW is the receiver BW [152]. Fig. 4.4 shows SNR and NF as a function of BW. For a given received power, the noise floor increases with receiver BW, in turn decreasing the SNR and the receiver sensitivity. NB and UNB modulations are capable of long-range due to

their improved receiver sensitivity and SNR from reduced BW. However, decreasing the receiver BW implies reduced transmit BW, leading to an increase in time-on-air and energy consumption. Thus, even in low data-rate applications, wireless systems operate at higher datarates to save battery life. To overcome the impact of narrow BW, existing LPWAN strategies limit the number of messages to reduce the total *time-on-air* [194].

Due to its reduced time-on-air WiChronos can operate in UNB without significantly increasing the energy consumption. The increase in time-on-air from UNB transmission of the anchor symbols is much smaller than that of the entire message (as in other LPWAN techniques). In our evaluation, we modulate the anchor symbols using BFSK in the 902-928MHz spectrum with a BW of 100kHz. RF modules such as TI CC1101 [191], CC1120 [195] can allow us to reach 10s of km with much lower BWs. Operating at the 902-928MHz spectrum also offers the advantage of mitigating multipath reflections and wideband interference. Devices operating in NB and UNB are unaffected by multipath as they experience no inter symbol interference [196, 197]. This is a physical layer phenomenon and we discuss this in our future work as an area of further analysis.

4.4.4 Medium Access Control

The third challenge identified in this work is co-existence in a large-scale deployment. In spite of the vast research on MAC protocols for large-scale [150, 198], ALOHA-based algorithms are implemented in LPWANs due to its simplicity. ALOHA allows a sender to transmit whenever it has data without any coordination between the senders. The simplicity of ALOHA makes it vulnerable to collisions in large-scale and/or heavy-traffic deployments. A packet collision occurs if one sender begins transmission during an on-going transmission i.e., twice the data transmission period is *vulnerable* to collisions. LPWANs using ALOHA-based MAC protocols suffer from collisions in large-scale networks when the channel is used for

transmission more than 20% of the time (on average).

WiChronos (by design) has low time-on-air and leverages the simplicity of ALOHA without getting penalized by collisions. **Data transmission time and time-on-air are different for WiChronos, unlike existing digital modulations.** As shown in Fig. 4.5,in current systems, the entire transmission is vulnerable to collisions, whereas, in WiChronos, only the anchor symbols are vulnerable, decreasing the probability of collisions. During the *data* transmission of one sender (T_{info}), the other sender can transmit their anchor symbols without affecting the on-going transmissions. We derive the probability of collisions given a node is transmitting a message following the textbook approach used in the analysis of ALOHA [199]. We assume a Poisson arrival process with a cumulative arrival rate of λ. Given a sender started a transmission, the event is a success if no other anchor is sent within $2t_{anchor}$.

$$\begin{aligned} \Pr(\texttt{collision}) &= 1 - \Pr(\text{no other event in } 2T') \\ &= 1 - e^{-\lambda 2T'}, \texttt{where T'} \ = t_{anchor} \end{aligned} \tag{4.7}$$

Fig. 4.6 plots the probability of collision for a given node *transmitting a 1-byte message every ten minutes* as a function of the network size. For SigFox, we assume its default overhead of 11 bytes at a datarate of 600bps and the shortest preamble allowed for LoRa with a spreading factor (SF) of 7, code rate 4/5 and 125kHz BW [200], operating in implicit header mode without CRC. We turn off CRC and MAC overheads, as well as ACKs in LoRa for a fair comparison. An arrival rate of 2λ is used in the calculation for WiChronos to account for the two anchor symbols.

With an increase in the number of sensors, the probability of collision for SigFox is the highest among compared technologies, due to its very low data-rate and very high time-on-air. The above parameters for LoRa are chosen for low-power and do not offer long range. For longer range, LoRa

recommends higher SF, which will lead to increased time-on-air, thus increasing the probability of collision. The rate of increase of probability of collisions with network scale is slower for WiChronos due to its reduced air-time. *It can achieve energy efficiency without limiting the number of messages and/or the network size.*. As shown in Fig. 4.6, reducing BW increases the probability of collision due to increase in symbol duration. However, this increase in collision is smaller for WiChronos as only the anchor symbol duration contributes to collision as opposed to SigFox or LoRa where the entire payload increases the collision probability. Therefore, we can leverage NB and UNB to improve range without significantly affecting scalability and energy efficiency. In a network of 1000 nodes, the probability of collision for SigFox and LoRa are 46.3% and 12.75% compared to WiChronos at 1.2% for a BW of 100kHz and 1.8% for 600Hz.

With increasing network size, the anchor symbol length will increase as log function of network size, since each sender is assigned a unique preamble and postamble as the local address. For example, a 2-byte anchor can address a maximum of 2^{11} senders each with a unique 16-bit preamble and postamble ($\frac{2^{16}}{2}$) and 4 initial bits for RF settling ($\frac{2^{15}}{2^4}$). The trade-off between network scale and energy efficiency will determine the anchor symbol length in practice.

4.5 Accuracy-Throughput tradeoff

The promise of long battery life and range in a large-scale is achieved at the cost of datarate. WiChronos achieves energy efficiency by offloading the communication burden to timers at the sender and the receiver and hence the data-rate of a link depends on the clock rate at the transceiver. Consider an MCU with a clock rate $f_c = 32.768\,\text{kHz}$. If increasing clock cycles each represent a value, a total of 32768 values can be conveyed in 1 s i.e., 15 bits ($\log_2(32768)$) can be communicated in one second(plus anchor

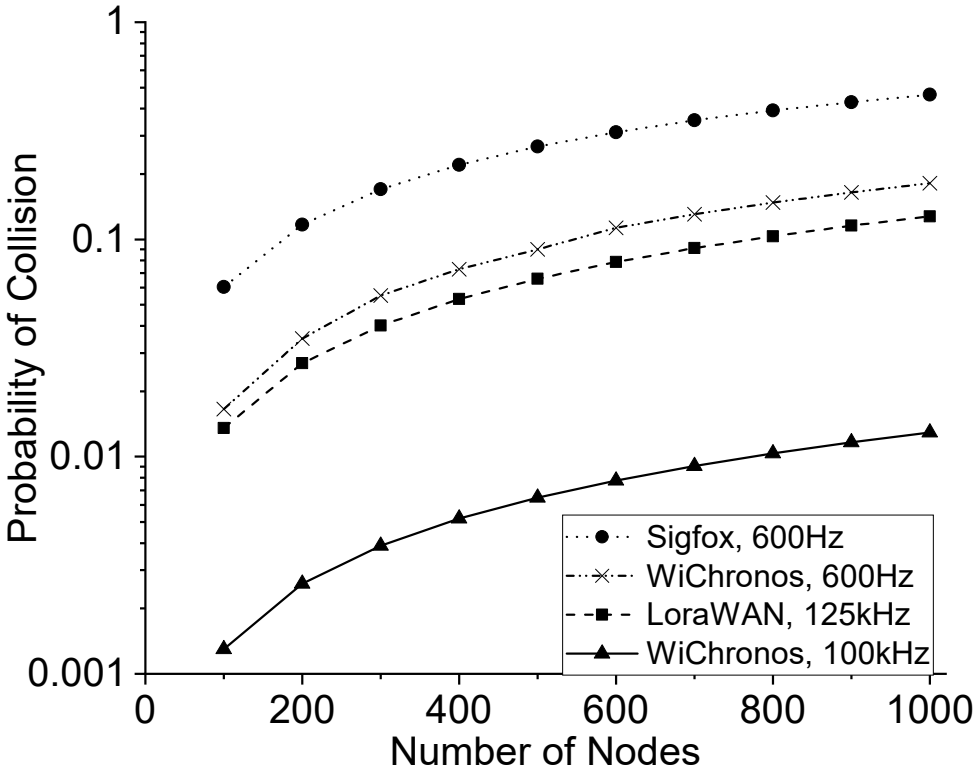


Fig. 4.6: Probability of collisions

symbol time). To generalize, the data-rate of a WiChronos link is given by

$$R_b = \frac{d \cdot f_c}{T_{info}}. \tag{4.8}$$

T_{info}, the time to transmit a "d"-bit message is in the range of $[0, 2^d - 1]$. For a uniformly distributed data source where the values of T_{info} are equiprobable, the expected value (average) of $T_{info} = 2^{d-1}$.

The achievable data-rate is lower than that of LPWAN technologies with comparable range. The numerator of data-rate in Equation 4.8 is a linear function of payload length while the denominator is an exponential function. This is in contrast with existing modulation techniques where the

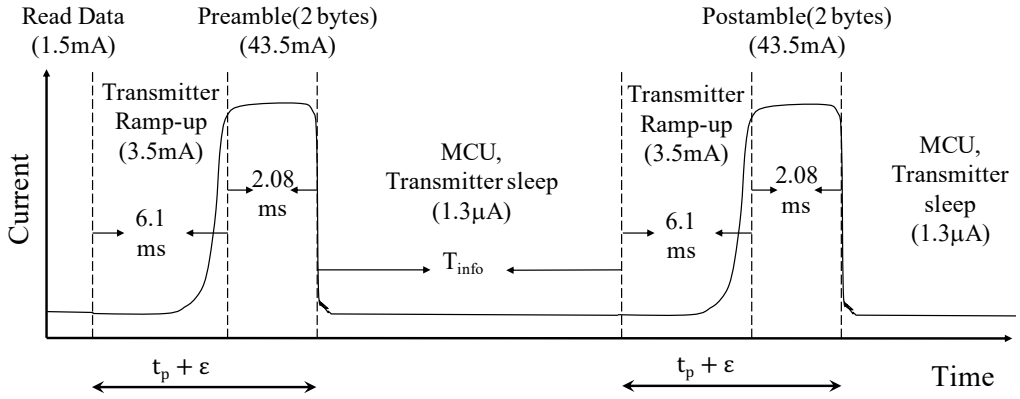


Fig. 4.7: Timing components of WiChronos sender

data-rate is a constant that is independent of the payload length. *WiChronos is thus not suitable for applications with high data-rate and low latency demands.*

4.5.1 Maximizing Data-rate

We present two strategies to improve our data-rate performance: [leftmargin=*]

Accurate higher clock rates

Efficient Time encoding. As shown in Equation 4.8, the data-rate of WiChronos is directly proportional to the clock rate f_c at the transmitter. Increasing f_c reduces the time between the anchor symbols for the same number of clock cycles and improve datarate. The accuracy of the clock plays a significant role in improving data-rate. Commercially available ultra low-power crystal oscillators [201], and MEMS clocks [202] offer high accuracy, high rate clocks. We will discuss the impact of clock skew on data-rate and accuracy later in the section.

The second strategy for improving data-rate is aimed at minimizing the average wait time between anchor symbols using apriori knowledge of the source distribution, analogous to source coding. The expected (average)

time to transmit a d-bit message is,

$$\mathbf{E} = \sum_{i=0}^{2^d-1} i \Pr(v(i)),$$

where $\Pr(v(i))$ is the probability of sensing a data value $v(i)$. Minimizing $\mathbf{E}$ will minimize the average time to send a value between 0 and $2^d - 1$, which will maximize the data-rate. This can be reduced to a continuous Knapsack problem [203], where the data values must be assigned a time value such that $\mathbf{E}$ is minimized. It has been proven that the optimum solution for continuous knapsack problem is achieved using greedy algorithm [203] i.e., arrange all possible sensor data in decreasing probability of occurrences and map to increasing time values in $[0, 2^d - 1]$. Mapping the most recurring data to the shortest time, we optimize the data-rate performance.

4.5.2 Timing Error Correction

The maximum achievable data-rate of a WiChronos link relies on the accuracy of clock rate, processing time, data transmission, and the propagation delay. Fig.4.7 presents a detailed timeline at a WiChronos transmitter. The currents and the duration listed are specific to the MCU and radio used in our prototype. By default, the radio and the MCU are in sleep mode. The total time to send data includes the radio wake-up time, the anchor symbol transmit time, and the information time. Timing errors in one or more of these components will affect the received T_{info}, leading to bit errors.

We broadly categorize bit errors in received data into the following categories,

errors in the anchor symbol,

anchor symbol loss,

processing and propagation time errors,

clock counting error. Existing error detection and correction mechanisms are designed for bit errors and require rethinking for timing errors. We propose a simple error detection mechanism for anchor symbol loss and correction mechanisms for bounded timing errors.

Anchor symbol error and loss

Though we choose the receiver bandwidth and anchor symbol length to minimize BER, there is a non-zero probability for anchor symbol error or loss. Existing coding techniques such as Hamming codes will be used to correct for single bit errors in the anchor symbol. Anchor symbol loss is detected using

timeout,

stateful receiver. We use the prior knowledge of the maximum payload length and the processing time at the sender to detect anchor loss using *timeout*. For each sender, the timeout value is set to $TO = t_{anchor} + T_{info-max}$, where t_{anchor} is the sum of maximum processing and transmission time to send an anchor symbol and $T_{info-max}$ is the maximum clock cycles mapped to a data. The receiver detects the loss of an anchor symbol whenever the counter exceeds TO. The second detection mechanism maintains the state of the anchor symbol reception for each sender. For every anchor symbol received, the receiver verifies the previous symbol received and the timer value is stored only if a postamble is followed by a preamble. Else, the counter value is discarded, reset and marked as an error, since recurring postambles (or preambles) indicate loss of a preamble(or postamble).

Processing timing error

In Fig.4.7, let t_p be the average time to send an anchor symbol. t_p is composed of the time to perform the operations in MCU such as ADC, timer setup, serial communication, enter and exit sleep mode, radio wake-up time, modulation, and transmission. Variations in the number of cycles to execute any of these operations can vary t_p in the range $[-\epsilon, +\epsilon]$. We assume that the operations in the MCU are deterministic and do not contribute to ϵ. The radio wake-up time can vary within a bounded range ([143].) We correct for this timing error by triggering the data timer after $t_p + \epsilon$. On reading a sensor data of *D*, the MCU sets a *transmit counter* for $t_p + \epsilon$ cycles and triggers the radio module to transmit the preamble. At the end of the transmit counter, the MCU and the radio are set to sleep mode for D cycles. By increasing the transmit time from t_p to $t_p + \epsilon$, the transmitter removes the variability in the preamble (and postamble) transmit time. The receiver counts the number of cycles between the preamble and postamble and subtracts $(t_p + ffl)$ to obtain T_{info}. We correct for variations in t_p by increasing the overall time to transmit as, $t_{anchor} \geqslant t_p + \epsilon$. For timing errors bounded by ϵ, the increase in anchor symbol duration from t_p to $t_p + \epsilon$ can achieve 100% error correction.

Clock cycle error

Timing errors due to clock skew at the transceivers can lead to incorrect T_{info} and hence bit errors. We propose a simple error correction mechanism that spreads out the data value (in time) to account for the clock skew. Consider the 32kHz crystal oscillator used in MSP430 FR2355. Though the quartz crystal oscillators have high stability, it has a tolerance of $\pm$ 30ppm, resulting in an error of $\pm$ 0.9Hz in room temperature [201]i.e., the measured clock cycle can vary by ≈ 1 clock cycle. To correct for this clock counting error, we assign data value D to clock cycles that are separated by

3 i.e., the minimum difference between two adjacent T_{info} transmitted over air is set to three, to correct for variations in the clock cycles measured. To generalize, when using a clock rate with a tolerance of $\pm\delta$, the minimum difference between two transmitted clock cycles is set to δ. Therefore, a sensor data D is mapped to $\delta + D \cdot (2\delta + 1)$. Using the above redundancy in time to correct for clock cycle errors will reduce the effective data-rate since fewer unique clock cycles represent data. Therefore, accurate(low tolerance) clocks are crucial to the design of WiChronos.

Propagation error

The time to receive an anchor symbol includes the propagation delay of the RF signal. At distances of a few *kms*, propagation delays of RF signals traveling at the speed of light are on the order of μseconds. Therefore, changes in propagation delays would also be on the order few μseconds. Error correction mechanism proposed above for clock skew is modified to correct for propagation errors too. A 50% error in propagation delay at a distance of 10 km can lead to an error of $\pm$ 0.8 cycles at a clock rate of 32 kHz. Apriori estimate of channel and propagation model is used to encode redundancy. For bounded error in propagation delays, we can achieve 100% error correction by further increasing the minimum difference between adjacent T_{info}. Combining these error detection and correction mechanisms, WiChronos can correct for all bounded errors and detect symbol losses.

4.6 Evaluation

4.6.1 Experimental setup

We implement WiChronos using Linx NT [143] as RF module and TI MSP430 FR2355 [78] for MCU as shown in Fig.4.8. Linx-NT has ex-

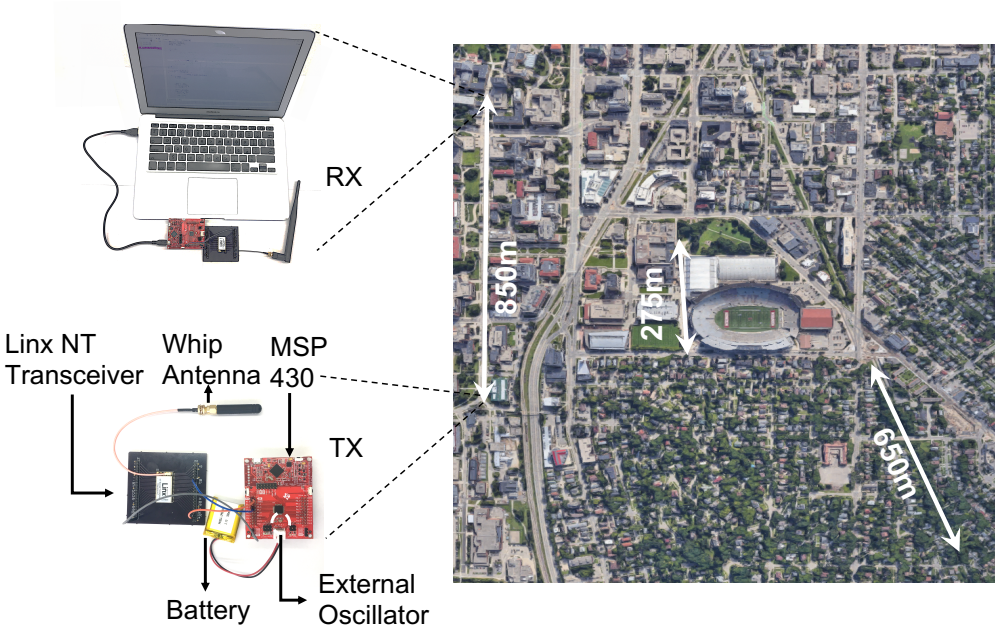


Fig. 4.8: Experiment locations and set up

tremely low sleep current(1nA), and a *transparent* mode without protocol overheads. The anchor symbols are transmitted at 9.6kBaud rate using BFSK over 100kHz bandwidth (BW) with a frequency deviation of $\pm$ 30kHz [143]. The MCU costs \$2.72 and the radio with antenna is \$45.8, bringing the overall cost to be $<$ \$50. Other less expensive transceivers such as TI CC1101 and CC1125 which cost below \$5 can also be used to implement WiChronos. Linx NT is chosen for its simplicity, allowing majority of the parameters to be set through hardware external pins. As part of our future work, we plan to explore various radio modules.

We use a 32.678kHz external crystal oscillator for data transfer (counting) as well as processing (MCU). Since information is encoded in the time difference, absolute clock synchronization is not needed. During system setup, the receiver stores the clock rate and anchor symbol of each transmitter. To understand the impact of timing errors, we estimate the maximum possible timing error analytically, verify it experimentally, and

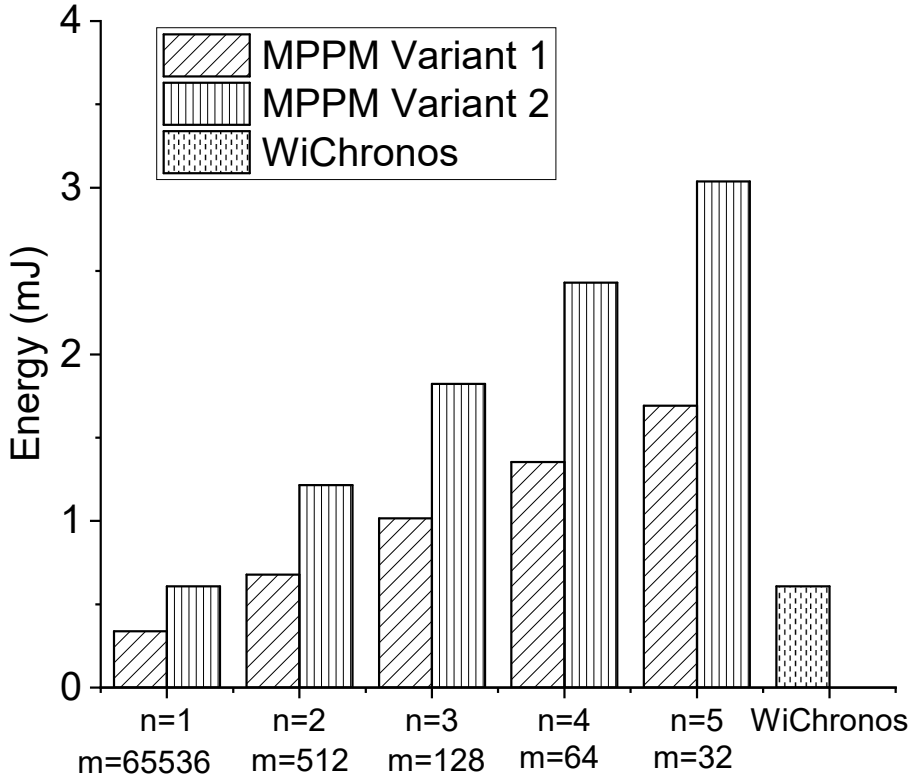


Fig. 4.9: Energy consumption of M-ary PPM and WiChronos

show that it is possible to correct all bounded errors (as explained in §4.5.2). We compare against LoRa experimentally and present analytical comparison with SigFox and M-PPM. Easy-to-program, Arduino based integrated LoRa module [204] (RFM69HCW) does not allow for energy management and has low battery life. We implemented an energy management module in SX 1272 [205] operated using MSP430; we reduce its preamble to 6 bytes, remove Cyclic Redundancy Check and MAC headers, disable ACKs, and set to transmit-only mode to minimize its energy consumption and provide fair comparison. Throughout this section, unless otherwise mentioned, we operate LoRa and Linx at 915.37 MHz center frequency. LoRa is implemented at a spreading factor of 7, coding rate 4/5 and BW of 125kHz.

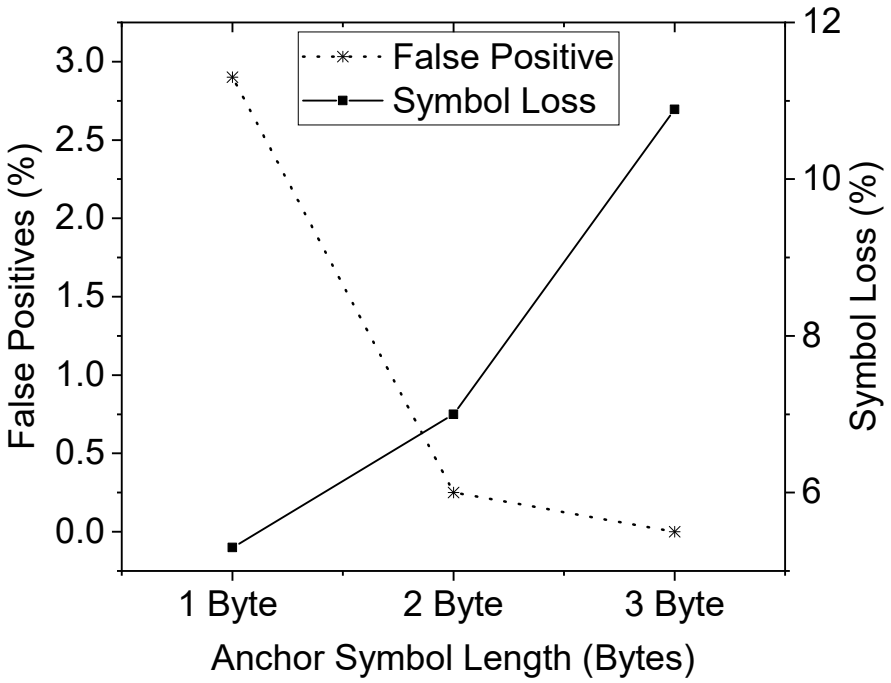


Fig. 4.10: Experimental verification of anchor symbol length

As shown in Fig.4.8, the sender is powered by a battery and the receiver is always-on. Both the transceivers use the external clock in the MSP and commercially available 1/4-wave whip antennas. Our implementation in MSP shown in Fig.4.2, circuit design, and hardware setup to recreate our results will be made publicly available*.

4.6.2 M-PPM Vs WiChronos

Following our discussion in §4.3, deploying PPM in a wireless system is challenging. Recently M-ary PPM has been considered for low data

*https://github.com/Yaman-Sangar/WiChronos

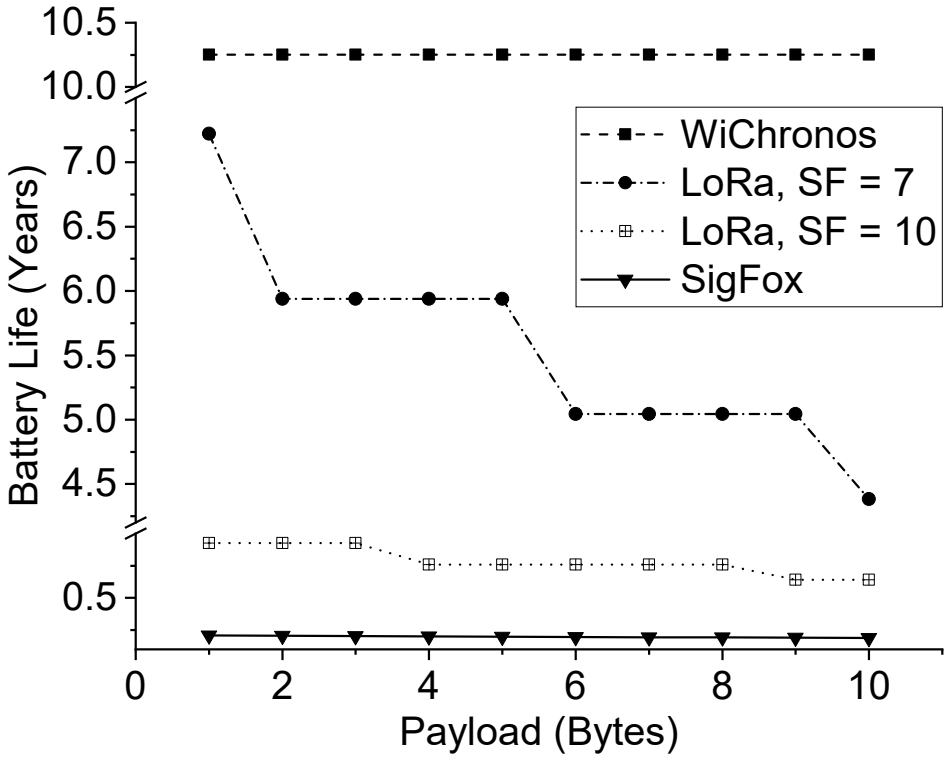


Fig. 4.11: Battery life of WiChronos Vs LoRa and SigFox

rate IOT networks [206]. WiChronos is a special case of the general PPM systems. In this section, we compare M-ary PPM against WiChronos on its energy efficiency, range, and scalability. MPPM encodes a d-bit message to one of 2^d symbols which are represented by **n** pulses in one of the **M** time slots. For example, in Fig.4.1, a 10-bit message is communicated using n=2 pulses in one of the M=32 slots [$\binom{32}{2} > 2^{10}$]. By transmitting these pulses over NB or UNB, long range can be achieved [206]. In the rest of this section, we assume a 100kHz BW for WiChronos and M-PPM pulses and therefore both the modulations can achieve the same range.

Unlike an optical system, a single pulse needs to be long enough for a wireless receiver to decode. Thus, the pulse length calculation follows

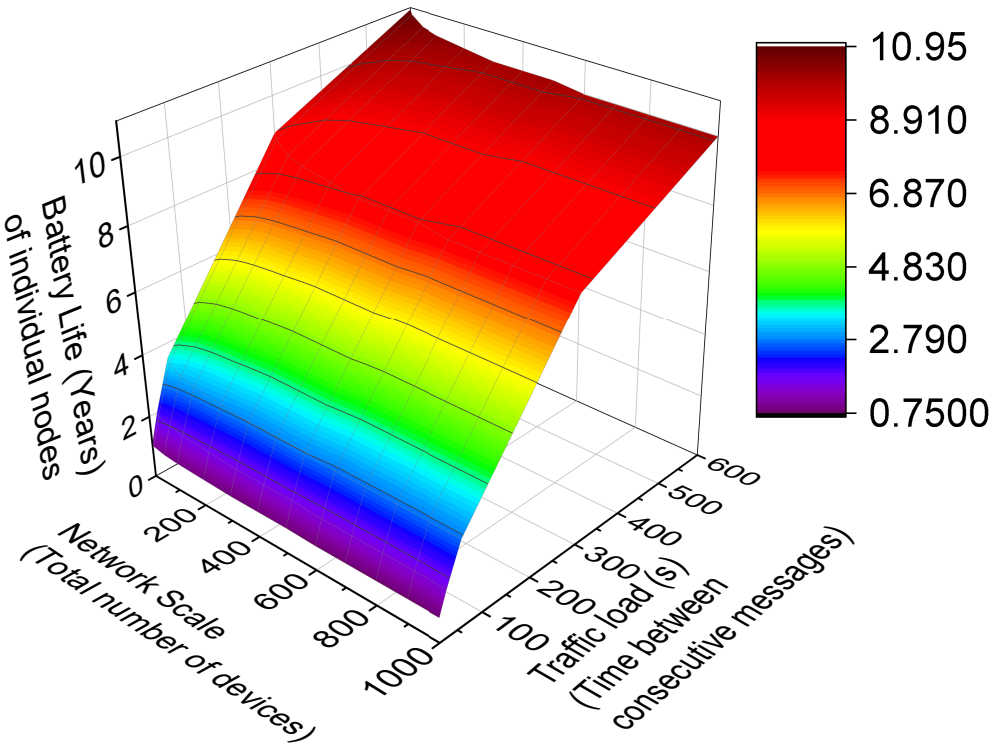


Fig. 4.12: Battery life of WiChronos Vs. scale and traffic load

that of the anchor symbol. We choose a 1-byte sequence of alternating 1s and 0s as a single pulse since that is the smallest length that can be communicated using Linx NT i.e., the shortest MPPM (and WiChronos) pulse is set to 8 bits. The start of a message is denoted by a 1-byte pulse, followed by the sender address, similar to a WiChronos anchor symbol. Shorter pulse lengths using other RF modules will benefit M-PPM as well as WiChronos. Our implementation of WiChronos uses 2-byte *anchor symbol*, where the first byte is used for synchronization and the second byte to identify the sender. Once an M-PPM receiver decodes the start of a message, it synchronizes the clock and waits for a pulse.The transmitter is in deep sleep mode when it isn't actively transmitting.

We implement the following two variants of MPPM that tradeoff energy and scalability.

Each pulse is 1-byte i.e. the shortest pulse. The short pulses consume lower energy, at the cost of MAC overheads. Since the receiver cannot differentiate pulses from multiple senders, a dedicated MAC protocol [188] or coding [180, 206] to coordinate transmission is required.

Each transmitter has a unique pulse. This eliminates MAC overheads but renders each pulse longer, like a WiChronos anchor symbol, trading off energy for scalability. Energy Consumption: Fig. 4.9 compares the energy consumption of WiChronos and the above variants of M-PPM, in transmitting a 2-byte payload. The energy consumption of WiChronos depends only on the length of the anchor symbols, while that of M-PPM increases linearly with the number of pulses n. For $n = 2$, the energy consumption of M-PPM is the same as WiChronos and requires M=512 slots to transmit a 2-byte message. While increasing n increases energy consumption, it decreases latency.
Scalability:An energy efficient M-PPM system (variant 1) would choose the shortest pulse, which will require MAC overheads and/or additional coding techniques to reduce collision rate. While a scalable M-PPM (variant 2) eliminates MAC overheads, it increases energy per pulse (similar to the anchor symbol of WiChronos), increasing the overall energy consumption and the pulse duration.
Data Rate: The frame duration of M-PPM is fixed for a given payload length i.e., M=32, with 2 pulses can encode 10 bits and always consumes 32 slots. WiChronos on the other hand, has variable message duration between the symbols that depends on the payload. WiChronos leverages lower data rate to achieve energy efficiency.

4.6.3 Anchor symbol length

In this section, we evaluate the robustness of our anchor symbol length design in §4.4.2. In our evaluation, we design the length to achieve an SNR $\geqslant$ 10 dB resulting in a BER of 10^{-3} for BFSK. At BER $= 10^{-3}$, we determine the optimum symbol length to be 10 bits, with a false positive probability $P_f \leqslant 0.01$ and symbol error probability $P_e \leqslant 0.001$ from Fig.4.3. Linx allows integer multiples of bytes (not bits) and hence we choose a 2-byte anchor symbol. The first byte is a sequence of alternating 1s and 0s to indicate the start of message and the second byte to identify the sender uniquely.

In Fig.4.10, we experimentally determine P_f and P_e for varying anchor symbol lengths. With increasing anchor symbol length, P_f decreases while P_e increases. At 2-byte anchor symbol, P_f is below 0.01 and P_e below 0.08. The experimental P_e is higher than the expected P_e derived in Equation 4.5 due to intermittent pedestrian traffic and strong winds. We present the impact of other environmental conditions on the symbol error rate later in the section.

From experiments we infer that the Linx-NT has a higher than average carrier sensing time, resulting in higher false positives. RF modules with smarter carrier sensing can further reduce P_f and hence the anchor symbol length. CC1125 [77] has a 4-bit settling time which can be reduced further by freezing the AGC setting for known input levels. In addition to that, the maximum transmit power of Linx-NT is 13.5 dBm while FCC allows up to 30dBm. An increase in transmit power and decrease in BW can improve SNR, reducing P_e which will allow us to reduce the anchor symbol length further. The presented result is thus an upper bound on the anchor symbol length and offers room for a further decrease in symbol length. *In the rest of our evaluation, we use 2-byte anchor symbols unless stated otherwise*. The receiver determines the preamble using correlation and starts decoding the address byte. A look-up table on the receiver is used to identify the

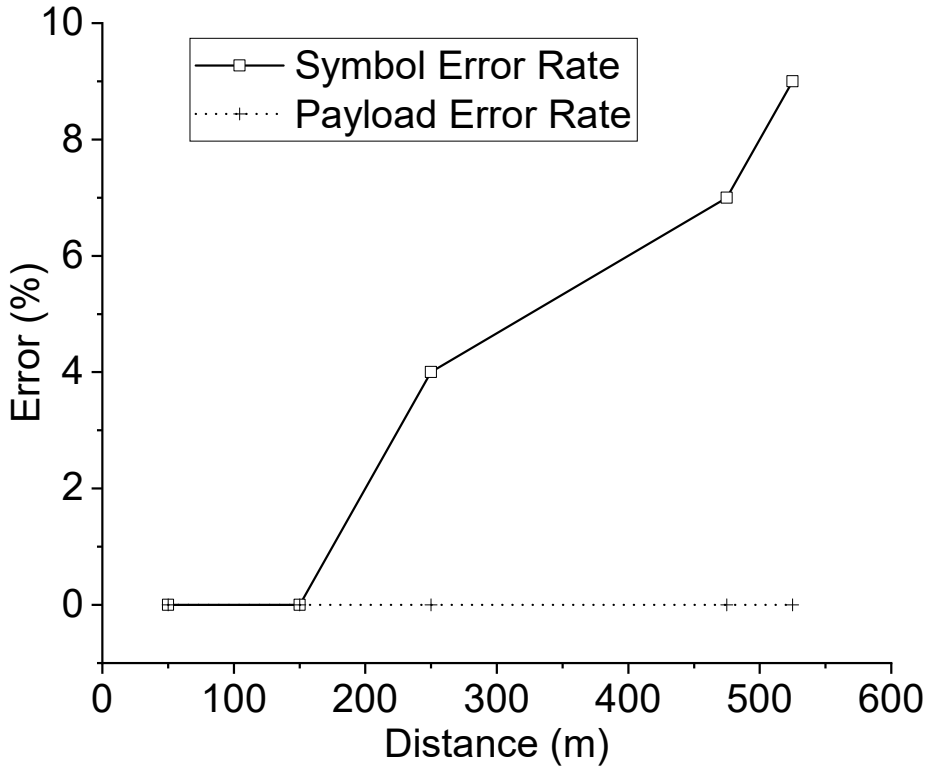


Fig. 4.13: WiChronos range

transmitter.

4.6.4 Energy Efficiency

We evaluate the energy efficiency of WiChronos with 2-byte anchor symbol and compare with LoRa and SigFox. The energy management module we implemented results in longer radio wake-up time. We experimentally measured the average radio wake-up time of Linx to be 4.2ms and that of LoRa $\leqslant$ 500µs. In Fig.4.11, we compare the life of a 250mAh, 3.3V coin-cell battery for varying payload lengths sent every 10 minutes. WiChronos has an impressive 10.25 years life for any payload length as its energy is only a function of the anchor symbol length. LoRa with SF=7 has a battery

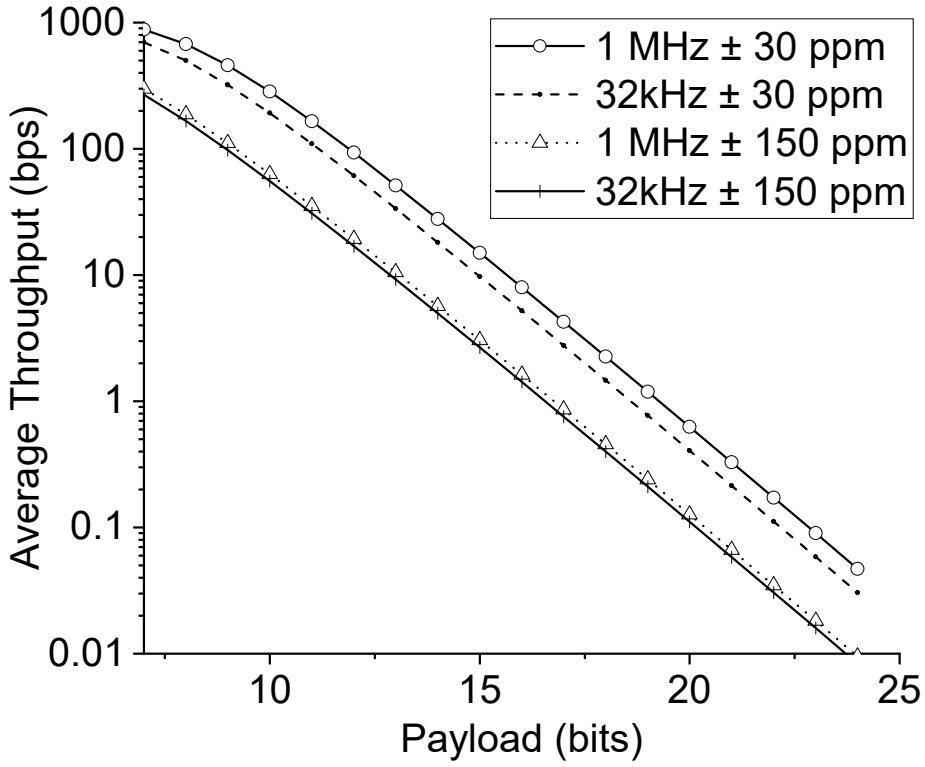


Fig. 4.14: Datarate performance

life of ≈ 5 years, but decreases with payload length. LoRa with higher SF used for longer range drastically reduces battery life (7 months at SF=10) while that of SigFox is the lowest at two months.

When transmitting a 2-byte payload, WiChronos reduces energy consumption by **1.7x** compared to LoRa-SF7, **11x** to LoRa-SF10, and **13.55x** to SigFox (BW normalized). The improvement in battery life, which increases with payload length, is due to, 1) reduced air-time 2) non-increasing energy-per-bit E_b. E_b for a WiChronos sender decreases with increasing payload as the overall energy remains constant while the number of bits increases. In classical modulation, E_b is constant and hence their energy increases with payload length. The energy efficiency will be further im-

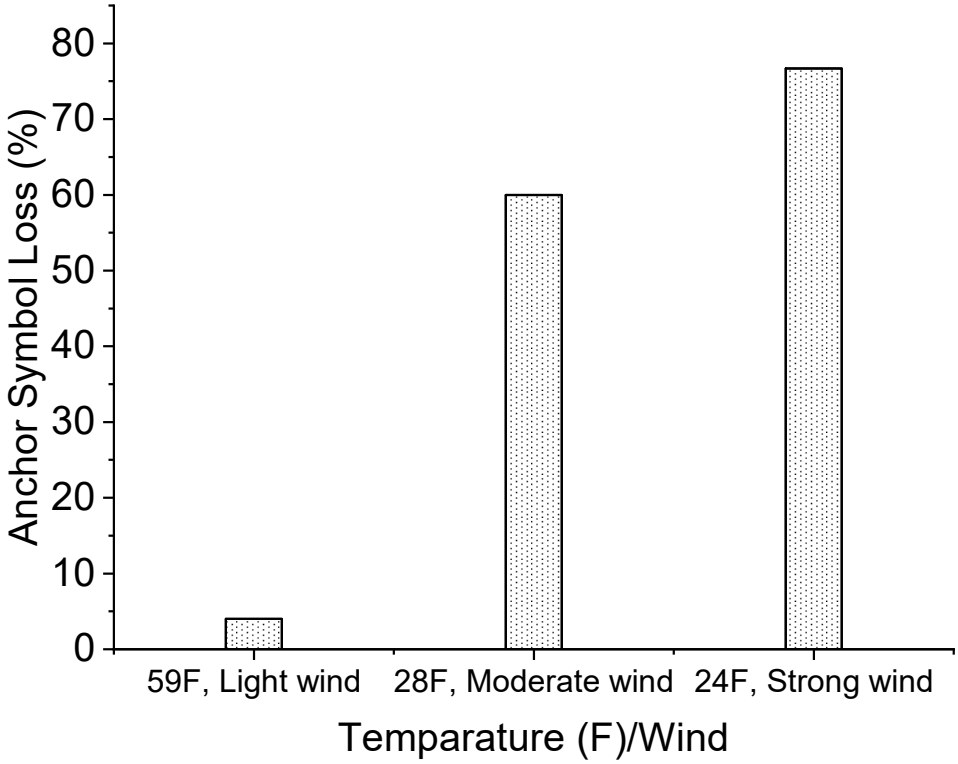


Fig. 4.15: Impact of environmental conditions

proved by using modules with smaller sleep currents and faster wake-up time.

The energy efficiency of WiChronos depends only on the length of the anchor symbol and the traffic load. Fig.4.12 shows the impact of traffic load and network scale on the battery life of a single node. For a given traffic load, battery life of a node decreases with increasing network scale, since the anchor symbol length increases with scale. The anchor symbol length is the sum of minimum decodable pulse (8 bits in this case) and $\log_2(NetworkSize) + 1$ to uniquely identify the senders. Similarly, with increasing traffic load, the overall time-on-air increases, in turn decreasing the battery life. At higher traffic loads where a payload is being sent once

every 15 or 30 seconds, the battery life reduces considerably as compared to low traffic scenarios. As discussed earlier, WiChronos derives energy savings partly from reducing the time-on-air which increases significantly when the traffic load and/or the scale increases.

4.6.5 Long Range

The long-range performance of WiChronos depends on the radio module and the modulation parameters used for anchor symbol. In §4.4.3, we derived the achievable communication range as a function of receiver BW. The maximum achievable range using Linx is limited to 914 meters, due to its reduced transmit power of 13.5 dBm. We verified the feasibility of long-range in indoor and outdoor environments using 1/4-wave whip antenna. Indoor experiments were performed in a 15 m x 10 m office space and along corridors up to 75 m long. Outdoor experiments were performed in streets with car traffic, bike paths with pedestrian traffic, and open fields at varying distances and weather conditions as shown in Fig.4.8.

Fig.4.13 plots the percentage of symbol and payload errors at varying distances for a 2-byte payload. The received symbol error remained below 10% at 525 m. At distances up to 850 m, WiChronos implemented on Linx was feasible under line-of-sight conditions. Payload error is the error in decoded data (time). On detecting an anchor symbol loss, the receiver ignores the data. In our experiments, timing errors remained bounded and therefore, payload error is zero, provided the anchor symbols were received correctly. This shows that under bounded errors, proposed mechanisms detect anchor symbol loss and correct timing errors with 100% accuracy.

SNR at the receiver can be improved by increasing the transmit power. RF modules with the maximum allowable Effective Isotropic Radiated Power(EIRP) and lower BW can reach distances of over 10 km [207, 77,

195]. It must be noted that the achievable range of our prototype is constrained by the hardware used here and is not an inherent limitation. Linx was chosen for proof-of-concept because of the ease of hardware programming it offers, simplifying communication between the MCU and the radio. The sleep current of Linx is extremely low which helps keeping the power budget down. Other RF modules such as TI CC1101, CC1125, CC1190 with UNB modulations have been shown to achieve 10s of km, using software programming. Any RF module with a protocol-free mode can be integrated with an MCU to implement WiChronos.

4.6.6 Error correction and data-rate

We identified four categories of error viz., anchor symbol loss, processing time error, clock skew error, and propagation error. The results presented in the rest of this section incorporate the anchor symbol loss detection. For the other three errors, we evaluate the data-rate performance of WiChronos, the accuracy of received data in the presence of timing error, and the impact of the proposed error correction mechanisms on data-rate. We implement the error correction mechanisms proposed in §4.5.2 at the transceivers.

Processing time error correction

Fig.4.7 shows the timeline of WiChronos data transmission, where the duration and currents are specific to the components used in our implementation. As discussed in §4.5.2, processing time error is corrected by elongating the transmission time t_p to $t_p + \epsilon$. For the system under consideration, $t_p = 196$ cycles and the estimated $t_p + \epsilon = 276$ cycles. At system clock rate of 32.678 kHz, the components of t_p with their corresponding average (A) and maximum (M) clock cycles are,

Radio wake-up time + MCU processing $(A{:}137\ ,\ M{:}200\ )$

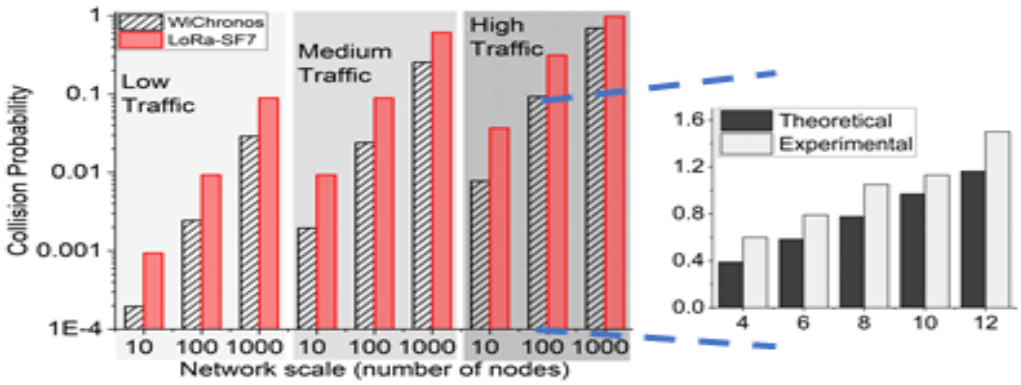


Fig. 4.16: Collision performance in a multiple access network

MCU processing (A:8, M:8)

2-byte anchor symbol transmission time at 9.6kBaud (A:51 ,M:68 . We estimate the upper bound of each operation to determine ϵ, and validated experimentally. On reading a sensor data, the MCU sets *TimerB* to count up to 276 cycles during radio wake-up and anchor transmission. The effective processing and transmission time is therefore a predetermined constant (276 cycles) and variations within this upper bound does not affect the measured T_{info} at the receiver. The receiver counts T_{info} and subtracts 276 to decode data, achieving 100% accuracy.

Table 4.3: Impact of Clock rate and skew on datarate

Clock Rate	Tolerance ppm	Tolerance cycles	Expt. Tolerance cycles
1 MHz [78]	$\pm$ 10000	$\pm$10000	$\pm$ 720
32.678 kHz [201]	$\pm$ 30	$\pm$ 1	$\pm$1
1 MHz [202]	$\pm$ 50	$\pm$ 5	Not validated

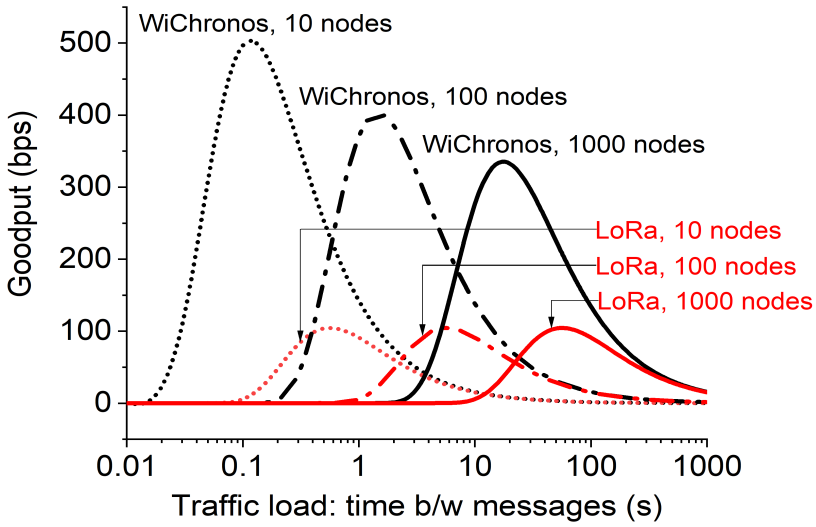


Fig. 4.17: Goodput Vs load for WiChronos & LoRa

Clock skew error

Clock skew directly affects the accuracy of the data received. We evaluate the performance of the two clocks present in MSP430 1) an external crystal oscillator (ECO) 2) an internal Digitally Controlled Oscillator (DCO) and analyse their impact on data-rate. Columns 2-4 in Table 4.3 show the clock rate and worst case tolerance of these clocks, along with other commercially available low-power clocks. Clock tolerance is an indicator of the accuracy of the clock. For example, with the 32.678 kHz ECO with a tolerance $\pm$ 30 parts per million [201] the measured number of clock cycles vary only by $\pm$ 1 cycle. We experimentally verified the tolerance levels of the ECO and the DCO by transmitting a predefined value of T_{info} every minute for over a week. Column 5 shows the tolerance determined experimentally for the ECO and DCO. Note that the theoretical tolerance values are an upper bound. Therefore, the clock skew correction proposed in §4.5.2 uses the tolerance values to determine δ. For the ECO, since $\delta = 1$, a data D

is mapped to $T_{info} = 3D + 1$. We correct for clock skew by introducing redundancy, which reduces the effective number of data values D that can be communicated, reducing the data-rate.

Higher tolerance requires higher redundancy for correction, negatively affecting data-rate. Fig.4.14 plots the achievable data-rate as a function of payload for different clocks. When using clock skew error correction, the tolerance has a higher impact on the data-rate than the clock frequency. For a given tolerance, the data-rate of WiChronos with 32kHz and 1MHz are comparable, due to the redundancy introduced for clock skew correction. Accurate clocks are key to the success of WiChronos. Low-power, high accuracy clocks in the order of MHz [202] can be integrated with the MCU to improve the data-rate performance of WiChronos. Note that the data rate decreases with increasing payload length, irrespective of clock tolerance, due to the exponential dependence of information time on the payload. Prior knowledge of source distribution can help with optimum data-time encoding to improve data-rate.

4.6.7 Multiple Access Control

In Fig. 4.16, we verify the effectiveness of WiChronos using ALOHA in a large-scale network under varying traffic load. We also experimentally validate the collision probability derived in Equation 4.7 in a network of 12 senders in heavy traffic scenario. We program the senders to wake up every 16 seconds to communicate a random 2-byte payload. Each sender is assigned a unique preamble and a postamble. On receiving valid bits on the serial interface, the MCU correlates the first byte to detect a packet and decode the second byte to identify the sender uniquely and trigger the corresponding timer. The senders are randomly placed inside a 15 m x 10 m office space. The presented results are averaged over a 2-day period.

We present the probability of collisions in a log scale Y-axis as a function of network scale under varying traffic conditions in Fig.4.16 The back-

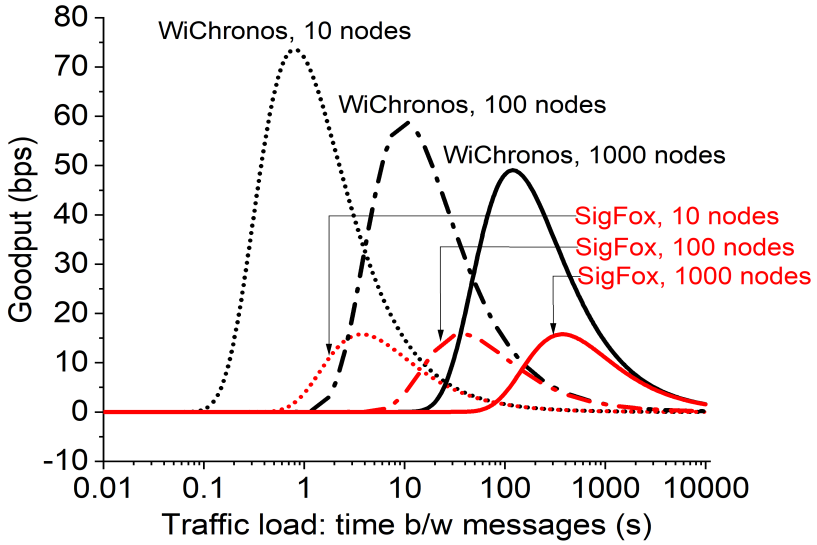


Fig. 4.18: Goodput Vs load for WiChronos & SigFox

ground grey shade darkens as the traffic load increases. We categorize the traffic load as high, medium and low when a 2-byte payload is sent every 15 s, 60 s, and 600 s respectively. As shown in Fig. 4.16, this probability in a 100 node network with high traffic is 9.1%, 31.3%, and 95% for WiChronos, LoRa with SF-7, and SF-10 respectively. At low traffic, this decreases to 0.24%, 0.93%, and 7.2% for WiChronos, LoRa-SF7, and SF-10 respectively. To compare against SigFox, we use a BW of 600Hz for both WiChronos and SigFox. For low traffic, collision probability is 1.6% and 60.3% for WiChronos and SigFox. Note that the collision probability increases with both network scale and traffic, due to larger volume of data, resulting in higher vulnerability to collisions. This increase in collisions is lower for WiChronos than that of LoRa and SigFox due to its reduced time-on-air. Since the channel is active only for the duration of the anchor symbols, the vulnerable period for collision of WiChronos is smaller for the same bandwidth and payload length.

We also validate the theoretical results with experiments for high-

traffic, small-scale network (zoomed-in image). The experimental results reflect the cumulative losses due to collisions, false positives, and anchor symbol losses. On an average, the theoretical collision rate is 75% of the experimental rate; the theoretical results are an approximation for a large scale network and we expect the experimental results to match theoretical for larger networks.

The reduced collision also improves the average network goodput performance (total number of successful data bits in the network in a given duration). We present the average network goodput as a function of traffic load for various network scales in Figs 4.17 and 4.18, where each transmitter sends a 2-byte message every *traffic-load* seconds. The above results are BW normalized for fairness, with WiChronos and LoRa using 100kHz and 125kHz respectively in Fig 4.17 and 600Hz for WiChronos and SigFox in Fig 4.18. Due to an increase in the volume of data, the goodput increases with traffic initially. However, it reaches an optimal point beyond which, collisions dominate and reduce the number of successful transmissions, inturn reducing goodput. For a given scale, the goodput of WiChronos outperforms LoRa due to its reduced collisions (Fig.4.16), and they converge at lower traffic. This is because, with reduced traffic load, data volume is low, inversely affecting goodput due to lower utilization of channel capacity. We compare the goodput performance of WiChronos and SigFox in Fig.4.18. As the scale increases, the increase in collision probability of SigFox is higher than that of WiChronos. Similarly, with reduced traffic load, the decrease in collision is higher for WiChronos, leading to a better goodput.

It must be noted that though WiChronos outperforms LoRa and SigFox in average network goodput, it trades off instantaneous goodput. In a 1000 node network where each node has a 2-byte payload every 10 minutes, the instantaneous goodput of a WiChronos and a LoRa node are 15.0 bps and 517.27 bps respectively. Similarly, with 600 Hz BW, the instantaneous

goodput of WiChronos and SigFox are 12.08 bps and 46 bps respectively. WiChronos is therefore best suited for applications with short payloads, where it can deliver low-energy over long-range in a large-scale.

LoRa can leverage the orthogonality of SF to enhance scalability [208]. Lower SF values offer high data rate, and low energy. High SF values help attain a greater range at the cost of data rate. While using different SF could help with scalability, it will also effect the range and battery performance. Another option offered by LoRa and SigFox is to use Frequency Division Multiple Access (FDMA). FDMA can be used in addition to ALOHA to further reduce the collision rate of WiChronos as well. For a given receiver BW, the reduced BW on each sender will increase the collision rate. However, this is only a function of the anchor symbols for WiChronos and the effect will be less pronounced compared to LoRa and SigFox. The decrease in collision rate from the reduced number of devices per channel outweighs the increase (Fig.4.6) due to lower BW.

4.6.8 Environmental Conditions

We evaluated WiChronos outdoors under varying weather and traffic conditions. Fig.4.15 shows the impact of temperature and wind on the anchor symbol error rate at a distance of 250m. SER increases by a factor of 15 at low temperatures and 19 when there are strong winds as well. While this is not a complete analysis, it indicates the strong impact of environmental conditions on anchor symbol loss, and in turn, bit errors at the receiver. We plan to explore the impact of environmental conditions and design antennas and protective casing to reduce the impact in our future work.

5 EXTENDING THE RANGE OF LPWAN USING AMATEUR RADIO SATELLITES

5.1 Introduction

87% of Earth's surface today, including oceans, deserts, forests, and glaciers is uninhabitable by humans [209]. Cellular coverage, primarily motivated by economics, has little incentive to extend coverage into uninhabited or sparsely inhabited regions. Environmental, ecological and geological studies [210, 211, 212] depend largely on data collected from these un-inhabited regions. While cloud computing and AI have provided unprecedented access to compute and modeling with a large amount of data, the lack of connectivity proves to be a significant challenge. Often, sensor data is stored locally on the device, and teams of humans are periodically (e.g., weekly or bi-annually) dispatched to physically collect sensor data.

Satellites, with their global coverage, can provide connectivity to these remote regions of the Earth. Today, satellite imaging-based remote sensing has emerged as a dominant alternative to ground sensing. The scope of satellite imaging, however, is limited and falls short in many areas e.g., seismic sensing, sensing under thick forests, and foliage. More recently, deemed as the "space-IoT" approach, several companies e.g., Swarm [30], Alen [213], Astrocast [214], Lacuna [29], Myriota [215] etc., have invested in launching Low Eart Orbits (LEO) satellites. Sensor devices on Earth now may transmit data directly to these satellites, which then relay it back to a ground station on Earth. Both satellite imaging and space-IoT, incur significant investment of launching satellites, building ground stations and obtaining spectrum licenses (when not using license-free bands). Consequently, connectivity and data obtained from it tend to be expensive, require reservations and is sparse and not real-time.

Our goal in this work is driven by the dream of democratizing near

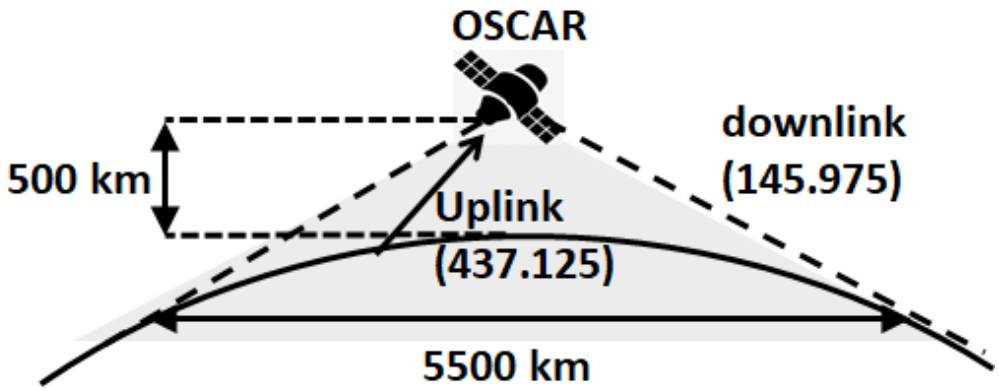


Fig. 5.1: How OSCAR Satellites Work

real-time IoT connectivity to cloud from anywhere on Earth i.e.,any scientist/researcher should be able to deploy a sensor anywhere on earth and obtain data from it without depending on the launching of dedicated space-IoT satellites. *Our contribution in this work is a novel approach to continent-scale IoT, SatConnect – that leverages pre-existing constellations of amateur radio satellites known as OSCARs* (*Orbiting Satellite Carrying Amateur Radio*).

OSCARs are built, launched, and used by amateur radio operators to primarily enable voice communication with each other through non-commercial satellites. An OSCAR satellite is typically equipped with a transponder relay that acts like a mirror in space – it simply shifts the frequency of incoming signals in a specific amateur frequency band to another and reflects it back without any physical layer processing (e.g., demodulation or decoding) (Figure 5.1). Any ham radio device that falls within the satellite's coverage area can receive this reflected transmission. For example, AO-73 [216] receives uplink radio transmissions in [432.125, 432.175] MHz, translates or shifts them to [145.975, 145.925] MHz, reflects them back to earth in the downlink over a coverage area of circle approxi-

mately 2500 kilometers depending on the height of the satellite. Currently, there are over a dozen operational amateur radio satellites orbiting Earth in the LEO belt. Thus, anyone with an amateur radio license may leverage an OSCAR satellite currently overhead and communicate with another device 2500 Km away.

The key idea behind SatConnect is simple – to leverage the OSCAR network of satellites to transmit IoT data to a receiver connected to the cloud potentially 1000s of Km away. Thus, an IoT sensor transmits its data over the amateur radio band. The OSCAR satellite then relays the signal over a large region that can be received by another device up to 2000 Km away, potentially connected to the cloud.

While, the idea is simple, there are several challenges to be overcome to make SatConnect viable. The primary requirement is that there must be no interference with ongoing voice transmission. The payload must be imperceptible and appear like white noise. This also requires the transmit power to be limited so as to not overpower transmissions from amateur radio users. Lower transmit power will reduce the SNR at the receiver and consequently, the packet error rate may rise. Robust modulation techniques are required to reduce packet loss. Due to the high velocities and large distances, the doppler shift causes variable drifts in frequency ranging from -7.5kHz to 7.5kHz. This shift needs to be corrected for to receive the payload accurately. The transmitter also needs to know when to transmit, therefore, scheduling uplink transmissions is yet another challenge in realizing SatConnect. For the nodes to know exactly when to transmit, they need access to the TLE of the satellites which is updated every 24 to 48 hours. Either the updated TLE must be accesible to the nodes or a schedule must be sent to them every few days to make sure the devices do not miss the short satellite access windows. We are also in need of protocols for a large number of devices to coexist within the coverage area. In this chapter, we explain these challenges and our solutions towards the

design and deployment of SatConnect.

5.2 Background

Wide area networks have seen tremendous growth in the last few years with the advent of low-power sensors, computing, and communication. With cheap, easy, and accurate sensing and monitoring easily available, the IoT market has expanded and wireless sensors are being employed virtually everywhere. At the same time, decades of research in infrastructure for space exploration has resulted in the ability to create nanosatellites like a cubesat, a satellite that can fit in a cube with and edge of an inch. Since communication distances of IoT devices are in the order of 100s of km, many technologies have used satellites to provide point-to-point communication across devices. Various attempts have been made in the past to build satellite clusters as the basis of the infrastructure for point-to-point communication between sensors. We list some of the prevalent ones today:

5.2.1 State-of-the-art space IoT

Lacuna: Battery powered sensors transmit data using a modified LoRaWAN protocol [45] to conserve power. This data is received by cubesats [29] launched by Lacuna and stored there for a short while, until it passes by a ground station on earth. The data is relayed from the ground station to the cloud platform for easy accessibility. Lacuna has deployed 5 satellites and the tags are in customer demo mode. A total of 240 LEO satellites have been planned for the Lacuna cluster.

Swarm: Data from various sensors is routed to a Swarm modem which is capable of storing 2000 unsent messages. The modem transmits it to a Swarm satellite, which is capable of storing 4000 messages, which relays it to a ground station. The data is available through various access methods. Swarm has launched 81 satellites of its planned cluster of 150 satellites.

Uplink frequency is 148-150 MHz and downlink frequency is 137-138 MHz. 750 packets (including both uplink and downlink) of 192 bytes each are allowed per month with options for extensions.

Astrocast: Astrocast nodes are a bidirectional module that is capable of transmitting and receiving from its nanosatellites. 20 of its planned 100 nanosatlellites have been launched and operate in the L band (1-2GHz).The satellites have a controlled lifetime of 3-5 years. The bidirectional communication protocol includes acknowledgements on reception as well as deployment of security patches and software updates. Astrocast guarantees a latency of less than 15 minutes and Astronodes consume 0.35W of power.

Myriota: Myriota allows 20 byte payloads to be transmitted from sensors to their LEO nanosatellites. This data is relayed back to a global network of ground stations and processed by software that is hosted in the cloud. A cloud API can be used to access this data. It offers 1250 messages per month and has options for higher data volume. Currently two of its 50 planned satellites have been deployed.

All of these technologies have spent millions of dollars to design, engineer, and launch their satellites. The design and construction of ground stations costs hundreds of thousands of dollars. Table 5.2 lists the power consumption of each ioT node, frequency of communication, and the number of satellites planned by these companies. While a larger number of satellites increases the probability that it will be visible to an IoT node, the expense that goes into designing and launching it cannot be ignored. We explain various types of satellites and their orbits and then discuss our proposed idea.

5.2.2 Satellite Altitudes and Orbits

There are three types of orbits that satellites can be launched at: high earth orbit, medium earth orbit, and low earth orbit. The height of the orbit, i.e.

the distance between the satellite and the surface of the earth determines the speed of the satellite. High earth orbit satellites are at a distance of 36,000km from the surface of earth and the satellite orbits at the same speed as earth. They stay at the same longitude but may drift in the north or south direction. These are also called geostationary satellites because they appear to be in the same place relative to ground. These satellites are extremely valuable for weather monitoring and various forecasting by gathering and sending information about cloud cover, wind speed and direction and humidity/water vapour. Given the relatively fixed location of the satellite, they are also useful for communication and are used to provide rescue and search beacons for ships and planes in distress. Geostationary satellites are also used to monitor solar activity and space weather and radiation patterns. It must be noted that geostationary satellites orbit right over the equator. Satellites in the medium earth orbit move faster at a distance of 20,200km from the surface of earth. They take 12 hours to complete an orbit and pass a given spot twice in a 24 hour period. There are two common orbits at this distance: semi-synchronous and Molniya orbit. The semi-synchronous orbit is a near circular orbit that is consistent and highly predictable. These properties lend well towards global positioning system (GPS) applications. The Molniya orbit is elliptical with the earth close to one edge. Hence, the satellite spends nearly two-thirds of its time over one hemisphere. They are helpful for communication in far north or south regions where geostationary satellites are unable to reach. Low earth orbit (LEO) satellites are at a height of 100km from earth's surface and take 90-100 minutes to complete an orbit. Most scientific and weather monitoring satellites are LEO satellites. These can have an equatorial orbit or move from one pole to the other. Polar orbitting satellites move on a sun synchronous orbit which means that whenever and wherever they cross the equator, the solar time on earth is constant. Regular adjustments are required to keep sun synchronous orbits consistent which allows them

to appear at nearly the same time in most locations on earth. In a 24 hour period, sun synchronous satellites usually view most of the earth twice, once in daylight and once in the dark.

5.2.3 Amateur satellite

Satellites that are built and used by amateur radio operators are called amateur satellites. Nearly all amateur satellites are LEO satellites operating in the unlicensed spectrum (144.1-148MHz, 420-450MHz) and are accessible to all users with a valid ham radio license. These satellites have linear or inverting transponders that up/down-convert a signal from one frequency band to the other. Since the transponders perform a direct frequency translation, they are agnostic to any encoding protocols that may be implemented. However, FCC requires that any information sent over these channels must not be encrypted. HAM satellites are typically used by HAM enthusiasts and are usually employed for voice communication, typically for recreational purposes, training to use a radio, and emergency communication. FCC regulations limit the transmit power on certain bands but geographical restrictions apply to the 420-450MHz band. FCC also limits the type of encoding on various bands. To the best of our knowledge, there are no encoding limitations to these amateur bands.

5.2.4 Constellations and connectivity

Table 5.1 lists various amateur satellites, the uplink and downlink frequency, the allowed bandwidth and the frequency of the continuous wave (CW) beacon transmitted by these satellites. There are over 50 satellites that are classified as amateur radio satellites. Since sun synchronous satellites cover large parts of the earth and appear at approximately the same time at a given location, we choose a subset of these satellites as presented in Table 5.1. AO-7, AO-73, and EO-88 have inverting transponders whereas

Table 5.1: Amateur satellite cluster proposed

Satellite	Uplink frequency (MHz)	Downlink frequency (MHz)	Bandwidth (kHz)	Beacon frequency (MHz)
AO-7	432.125 - 432.175	145.975 - 145.925	40	145.975
CAS-6	435.27 - 435.29	145.915 - 145.935	20	145.910
CAS-3	435.030 - 435.050	145.665 - 145.685	20	145.660
AO-73	435.150 - 435.130	145.950 - 145.970	20	145.953
EO-88	435.015 - 435.045	145.990 - 145.960	30	145.940

CAS-6 and CAS-3 have linear transponders. We find that this small subset of all amateur satellites is capable of covering most of the United States of America. It must be noted that not all amateur satellites are accessible worldwide. In fact, most of the American amsats can be used only by licensed users within America. Various other countries have similar rules too.

Since amateur satellites are already in orbit, we propose using these as the basis of the infrastructure required to communicate from remote locations. Since the primary purpose of amateur satellites is voice communication, any data that is transmitted must appear like white noise to any active radio operators. Active data transmission from an IoT node to a ground station must not disturb any ongoing voice communication. We propose encoding data as a Binary Phase Shift Keying (BPSK) signal and modulate it using Direct-Sequence Spread Spectrum (DSSS) using the Hamming(7,4) code to distribute the signal power across the entire bandwidth.

5.3 System Architecture

The three primary components of SatConnect are the transmitting IoT devices, satellites, and the ground station to receive. We leverage the OSCAR satellite network that is agnostic to any modulation. In this section,

Table 5.2: Existing technologies for global IoT connectivity through satellites

Company	Number, type of satellites planned	Frequency (MHz)	IoT node power consumption
Lacuna	240	2.4GHz	–
Swarm	150	148-150MHz (Uplink) 137-138MHz (Downlink)	3.15 - 3.6W
Astrocast	100	1-2GHz	0.35W
Myriota	50	399 - 403MHz (Uplink) 400-401MHz (Downlink)	1.8-1.9W

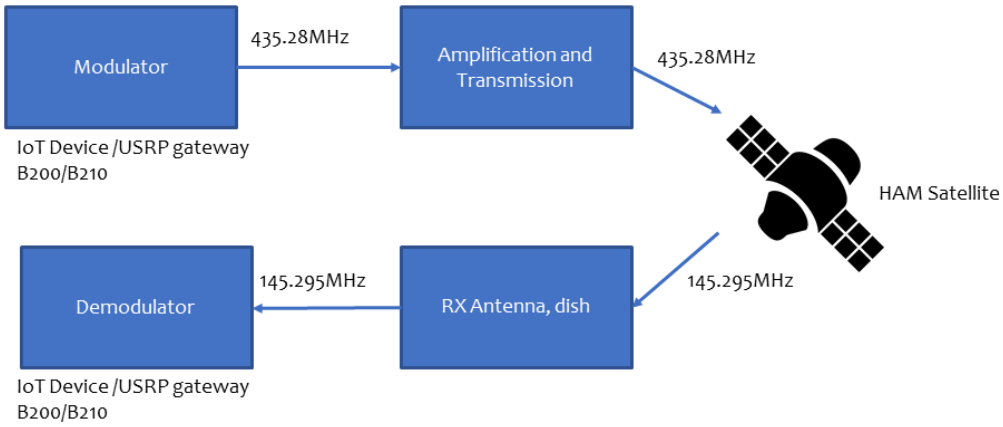


Fig. 5.2: Block diagram

we describe the system architecture of the transmitter as well as the ground station.

The transmitter in SatConnect consists of the radio front end, power amplifier, and antenna. Most of the OSCAR satellites use an uplink frequency in the 430 - 440 MHz band with a bandwidth of 20kHz and hence, the transmitter must adhere to this frequency and bandwidth limit. Further, satellites also stipulate the maximum power they can receive. If the power received by the satellite is higher, the transponder will saturate and the data will be lost. Hence, it is crucial to study the link budget of the transmit path and design the transmitter accordingly. Power amplifiers

may be required to meet the required transmission EIRP. It must be noted that power amplifiers have limitations on the input power to the device. Careful consideration must be placed upon choosing the radio and power amplifier to make sure that they are compatible with regards to the output and input power limits respectively. We explain these design choices in more detail further in this section.

The output of the power amplifier is transmitted to the satellite through an antenna. Most OSCAR satellites are equipped with a whip antenna or a right/left handed circularly polarised antenna. Whip antenna is omni-directional which makes the placement of the antenna straightforward but usually the gain of the antenna is much lower. The transmitter can use any antenna to send to a satellite with a whip antenna. On the other hand, a circularly polarised antenna requires careful positioning such that the antenna points towards the satellite at all times. It is also important to make sure that the direction of polarization of the antenna matches that of the satellite. Though a whip antenna can be used to transmit to a satellite that has a circularly polarised antenna, there will be a 3dBi attenuation to the signal because of the antenna mismatch.

The satellite receives the signal from the transmitter and amplifies it. The signal is then downconverted (upconverted) from the 440MHz (144MHz) band to the 144MHz (440MHz) band. This signal is amplified again and then transmitted back towards earth.

Once the data is reflected back from the satellite, it is received at a ground station located 1000s of km away. Ground stations often uses a dish to provide substantial gains of over 20dBi to improve the SNR of the received signal. The size of the dish depends on the frequency of the received signal; for a signal in the 144MHz band, a dish would have a diameter of about 1m or more. However, dishes increase the cost of the ground station and are not necessary for LEO satellites. Whip antennas are often used at the receiver, though some satellites use circularly polarised

antennas to reflect the signal back. In such a case, the receiver incurs a 3dB loss. Most omnidirectional antennas would be fine but the gain would vary and given the high path loss, a high gain antenna is preferable. An alternative way to increase the SNR is to use a low noise amplifier on the ground station. Since the ground station receives weak signals that are just above the noise floor (or sometimes buried under the noise floor), a low noise amplifier is needed to amplify the signal without amplifying the noise. The LNA can provide up to 20dB of gain while raising the noise by only 3dB[]. Any receiver that is capable of receiving at 144MHz (or 440MHz) can be used. Although we use a software defined radio as our transmitter and receiver, any radio that can support the chosen modulation in the 144/440MHz frequency band over a 20kHz bandwidth can be used. We present the choice of modulation and other design parameters in the next section.

5.3.1 Choice of Modulation

The choice of modulation that can be used impacts signal audibility and noise resilience. FCC has regulations that govern the type of modulations that are allowed in various frequency bands. While staying within these bounds, it is crucial that any background voice communication that is ongoing should not be disturbed. Therefore, data must be modulated such that it appears as white noise to any ongoing voice communication. Several modulations such as FSK and ASK that rely on bits being encoded to specific frequencies are not possible because these appear as a constant and audible tone. Reducing the power of the signal reduces its audibility, but it also results in a lower SNR making detection and demodulation prone to more error. Since data bits cannot be encoded to a single frequency, each bit would have to be encoded by spreading the power over several frequencies. Spread spectrum modulations are required in order to make sure that there is no perceivable disturbance to users engaged in using the

spectrum for voice communication. The overall signal power is spread across the spectrum so that the power per frequency is low.

We propose two spread spectrum techniques to modulate data: chirp spread spectrum and gold code sequence. Gold code sequence: A gold code is a binary sequence with low cross correlation and high auto correlation property. We use three unique gold codes, one each for the preamble, bit 0, and bit 1. Each sequence is defined by the number of chips (n) such that the length of the sequence is 2^n. For example, a 10 chip gold code consists of a sequence of length 1024. We follow the following steps to encode the preamble and data bits using the gold code sequence: first, we divide the bandwidth into as many pieces as the length of the gold code. When the bandwidth is not an even multiple of the length, we reduce the bandwidth to find the largest value that is an even multiple of the length. This splits the bandwidth into evenly spaced frequencies. For a 10 chip code (length of 1024), we choose the bandwidth to be 19.456kHz (this gives us 19Hz between two consecutive frequencies). This creates a one-to-one correspondence between each bit of the gold code sequence and a specific frequency within the 20kHz bandwidth. We then create a time domain signal by choosing the frequencies that correspond to 'bit 1' in the gold code sequence. Since a unique gold code is used for the preamble, data bit 0, and data bit 1, we get three unique time domain signals. We detect and demodulate the received data by correlating each bit with the stored time domain signal for bit 0 and bit 1. Since gold code sequence has a strong autocorrelation and weak cross correlation, we observe a strong peak only when the received bit and the stored bit are the same. By choosing gold code sequences that are not balanced (unequal number of 0s and 1s) in favour of sequences that have a greater number of 1s, we can spread the signal power across a larger number of frequencies. Alternatively, if the received signal strength is low, gold codes with a smaller number of 1s can be used to increase the power per frequency.

CSS: A chirp is a sequence where the frequency increases (up-chirp) or decreases (down-chirp) linearly with time. CSS has been used in LoRa[] and is a popular choice of modulation to achieve long communication range. We define the number of unique frequencies in a chirp as its Modulation Order (MO). Data is encoded by changing the starting frequency of the chirp. Since there are a total of MO starting frequencies, each chirp represents $log_2(MO)$ number of data bits. A base up-chirp (down-chirp) stars at the lowest (highest) frequency and ends at the highest (lowest) frequency as dictated by the available bandwidth. The received chirps are demodulated by multiplying them with a base down chirp. This concentrates all the signal power on a single frequency which is the starting frequency of the chirp. Data can be decoded once the starting frequency is known. Since CSS uses the entire channel, it is resilient to channel noise. Therefore, chirps that are buried under the noise floor can also be detected and demodulated. Hence, even in low SNR conditions, chirps can be received, demodulated, and decoded which offers a significant advantage over gold codes.

The received signals from the satellite are prone to immense doppler shifts. The satellite and earth move at high speeds which results in frequency shifts of up to -7.5kHz to 7.5kHz when the satellite moves from one horizon to the other. Demodulating a gold code based packet in the presence of doppler shift poses additional challenge of doppler detection and correction. We explain our doppler correction process in Sec5.5. We explain the CSS packet structure in further detail in Sec5.5.

5.3.2 Choice of hardware

Most LEO satellites are at a distance of 100km from the surface of the earth. Given the prior knowledge of the transmit frequency, we can calculate the total path loss that the transmitted packet will incur. For example, transmitting a packet to CAS-6 incurs a path loss of 140dBm. Since the

maximum transmit power of most radio front ends is less than 20dBm, a power amplifier is needed to boost up the signal power. Cables connecting the radio to the power amplifier and the antenna add to losses. For instance, we determined experimentally that a 1m cable connecting the transmitter to the power amplifier had 2dBm loss. Most satellites specify the EIRP of the transmitted signal to be at least 40dBm in order to reach the satellite but not saturate the transponder. As long as the power levels are met, any radio that supports the chosen modulation can be used as the transmitter.

5.3.3 Coexistence with other tags

When multiple tags transmit packets simultaneously, there will be collisions which results in packets getting lost. Since the path loss across all of these packets is very large, all the received packets would be expected to have low SNR at the receiver. Several techniques to resolve collisions between LoRa packets have been proposed. These techniques could be leveraged to improve the system scale up to 100s of devices.

5.4 Sensor Node Scheduler

We have discussed the choice of hardware and modulation as well as the limitations of bandwidth. However, one key question that is still unanswered is 'how does the transmitter know when to transmit?' In order to enable low power operation, the microcontroller on the sensor node maintains the sensors and the radio in low power mode. The microcontroller has to be informed when the next satellite pass would be. One way to do this would be to send the information about the next satellite pass as a response to the packet sent by a node. There are several challenges associated with this approach: the received packet from a satellite is on a different frequency so the node needs to have a 144MHz antenna and the appropriate matching circuit and an LNA to be able to receive this

information. The added hardware and use of the radio increase the power consumption significantly. An alternative approach is to choose specific satellites that a specific node could communicate with. Each satellite transmits a beacon at a unique frequency; it is usually one of the starting or the ending frequencies of the allocated bandwidth. We propose using a low power wake up receiver tuned to specific beacon frequencies to detect the presence of the chosen satellite passing by. As soon as the microcontroller detects the presence of the satellite, it can transmit its payload. To make sure that the payload was transmitted, the MCU waits to receive at least one more beacon signal from the satellite. If the MCU does not detect a beacon, it assumes that a part or all of the data was not transmitted and resends the packet at the next available satellite pass. This technique can be further upholstered by using sun synchronous satellites. Sun synchronous satellites pass by at a given location at approximately the same time every day. This gives the MCU a coarse grained idea of the time at which it will have access to the satellite.

5.5 Implementation

In this section, we describe the hardware and software we used to implement SatConnect. To be able to experiment with different modulations, we use USRP B200 as the radio front end to transmit and receive the payload. GNURadio is used to interface with the USRP and implement filters. We implement two modulations, gold code and CSS, on MATLAB to generate samples that the USRP transmits. We use a power amplifier to increase the transmit power of our sender to 35dBm. A V shape dipole antenna is connected to the output of the power amplifier to transmit the payload to the satellite. All of the OSCAR satellites have vertically polarized antennas (other than those with circularly polarized ones). We use the V dipole antenna in a vertical configuration to align the polarization with that of

the satellite. Not doing so will result in a 20dB loss and nothing will be received from the satellite. Once the signal is downconverted and reflected by the satellite, it is received at another V shape dipole antenna tuned to the receiver frequency. The antenna is connected to a low noise amplifier (LNA) which provides a 12dB gain to the received samples. These samples are then fed to the USRP, filtered to a bandwidth of 50kHz using GNU-Radio, and stored to be demodulated and decoded on MATLAB/Python. All our codes on MATLAB/Python as well as GNU radio sketches along with more details on the hardware set up are made publicly available.

We implement gold code and CSS modulation to transmit data. The bandwidth for both of these modulations is 20kHz. We explained the reasons for choosing these modulations in Sec5.3. Data is modulated by choosing frequencies from a given preamble/bit '0'/bit '1' gold code that correspond to a value of 1. Once we have our time domain signal values, we create a packet that consists of 3 preambles followed by a stream of 100 randomized bits. Upon reception, there are three steps to demodulation and decoding the received samples: coarse grained preamble detection, determination of the start of data packet, and finally, decoding the received samples. First, we choose two consecutive windows such that each of them has the same number of samples ($N_{Samples}$) as we expect in the preamble/bit '0'/bit '1'. We then autocorrelate these windows and store the result in an array. We move both windows up by $N_{Samples}$ and then perform autocorrelation again. Having three preambles guarantees at least one position where both these windows will be within samples from the preambles and will result in a high autocorrelation peak. Once an autocorrelation peak is detected, a coarse-grained position of the preamble is known. This completes the first step of demodulation. The next step is to detect the start of frame delimiter (SFD) to be able to identify the precise sample that represents the beginning of the first payload bit. To do so, we slide the window one sample at a time (instead of sliding it

by $N_{Samples}$ for coarse grained preamble detection). At each point, we crosscorrelate the window with the stored preamble. The position where we see a peak in the crosscorrelation output represents the position where the window is exactly aligned to the preamble. We then apply a frequency shift from -7.5kHz to 7.5kHz in steps of 1Hz to the stored preamble and crosscorrelate the shifted version of the stored preamble with the received one. The frequency shift that gives a peak at the crosscorrelation output represents the doppler shift of the signal. Once the SFD and doppler shift have been determined, the next step is to decode the payload and convert it to bits. Starting at the SFD, we choose a window of size $N_{Samples}$ and crosscorrelate the window with the stored bit '0' and bit '1' samples that have been shifted by the doppler shift that was calculated above. The crosscorrelation results in a peak which determines if the payload peak is 0 or 1.

We also implement CSS modulation in a format similar to a LoRa packet. The payload consists of a preamble consisting of 8 base upchirps. We choose the modulation order (MO) as 16, 32, and 64. Based on the choice of MO, we encode the payload bits to chirps. The starting frequency of the chirp is modulated by the payload. Once the packet is received, demodulation is performed by multiplying the received chirp with a downchirp, taking the FFT of the product, and locating the bin that the FFT peak is in. The bin frequency corresponds to the data, hence data can be easily decoded once the bin frequency is determined. In the presense of doppler shift, the bin frequency is shifted. The doppler shift is determined from the preamble. The preamble is defined as a chirp whose starting frequency is the first frequency in the bandwidth. hence, the observed preamble bin frequency is the value of doppler shift. We subtract this value from all the other received bin frequencies before decoding the data.

We use both of these implementations in our experiments using ISS transponder as our choice of OSCAR satellite. We describe the experimen-

tal set and results in detail in Section5.6. I am still performing experiments using the CSS modulation and don't have enough data to present a statistically robust result just yet. I will update my results here as soon as I have collected data from at least 1000 packets.

5.6 Evaluation

In this section we present an evaluation of our prototype as described in Sec. We evaluate our prototype across the following fields: Audibility of transmitted data: We evaluate if the modulated data appear as white noise to users using the spectrum for voice communication through a user study. Bit error rate: We evaluate the bit error rate for different gold code sequences used to modulate data by changing the chip length of the gold code sequence.

5.6.1 Audibility of transmitted data

Since the primary use of Ham satellites is voice communication, it is imperative that any ongoing use of the spectrum for voice transmission is not impacted negatively. In order to study this, we conducted a user study to understand the effect of the presence of modulated data in background. We had a pool of 8 users of which 2 were female and 6 were male. Their age ranged from 19 to 34 and none of them had any experience with voice communication through HAM radios before. Each user was given a set of 200 randomized sessions. These 200 sessions consisted of 25 sessions each where there was no background transmission, gold code modulated data transmission with chip length of 8, 16, 32, 64, 128, and chirps with spreading factor 7 and 9. These 25 sessions with background data of a particular modulation consisted of 5 sessions each where the interference signal power was sent at low, medium, and high receiver SNR. Two low SNR (3-5dB and 6-8dB) transmissions, two medium SNR (12-15dB, 18-

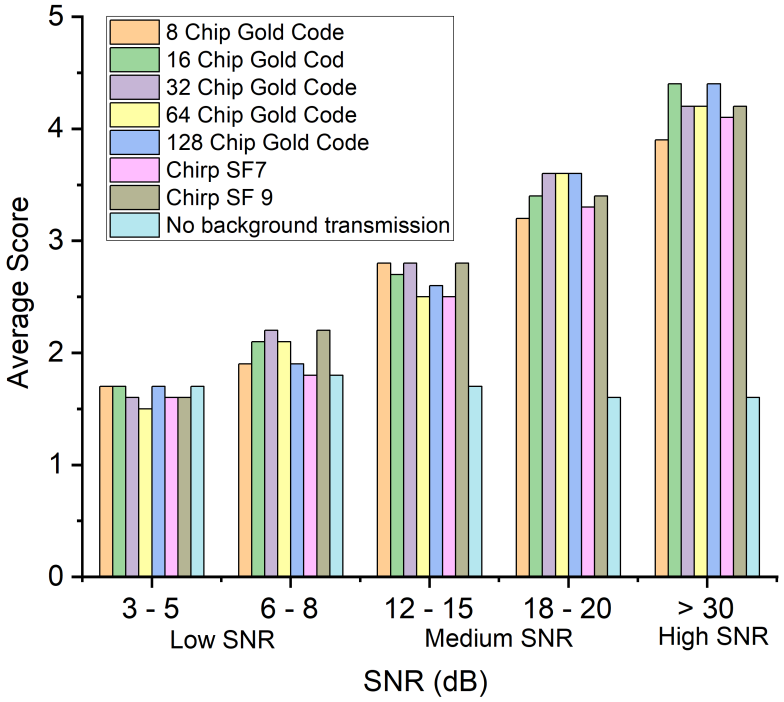


Fig. 5.3: Average user response for various modulations across different SNR conditions

20dB) transmissions, and one high (over 30dB) SNR transmission was used. All the users were given a hand held HAM radio that was set to receiver mode. Eash 'session' with a user lasted 30 seconds at the end of which the user was asked to rate the quality of the voice communication as a comparison to a baseline. The baseline was defined as a 30 second conversation with the user when they were told that no background transmission had been initiated. In all the other sessions except when the users asked for a baseline, the users were not told if there was a background transmission happening or not. All users were asked to rate the quality of the conversation according to the following scale: 1: Better than base-

line, 2: Same as baseline, 3: Little worse than baseline, 4: Much worse than baseline, and 5: Inaudible. Based on the responses from the users, figure5.3 plots the average responses across all users across all sessions on the x axis and the SNR of various interferring modulations on the y axis. From Fig5.3, we notice that all modulations at low SNR background transmission do not appear as a disturbance to the users. Since the average score is between 1 and 2, users do not perceive the ongoing communication to be any worse than the baseline. As we increase the interference power to medium and high SNR scenarios, we notice that the channel interference becomes more audible. The user study concludes that at low SNR, the channel interference due to background date transmission is imperceptible.

5.6.2 Bit error rate

In this section we evaluate the bit error rate of the gold code sequences of chip length 8, 16, 32, 64, and 128. We used the transmitter and ground station prototype as described in Sec5.5. 200 packets each with 100 data bits were transmitted for each chip length. In Fig5.4 e plot the bit error rate on the x axis and the modulation on the Y axis. BER is lower when the chip length is lower. This is because when we reduce the chip length, we reduce the number of 1s in the gold code sequence. Since the signal power is constant, the per frequency power is higher and therefore, the per frequency SNR is higher.

Further analysis of CSS modulation is currently the focus of my experiments. I will present results on the packet error rate of CSS modulation at three different modulation orders (16, 32, and 64). I will also perform a long range experiment where the transmitter and receiver are separated by 1100km and present the packet error rate for chirps using different modulation orders (16, 32, and 64). I will also use the data collected to plot the data rate at different spreading factors and study how the data

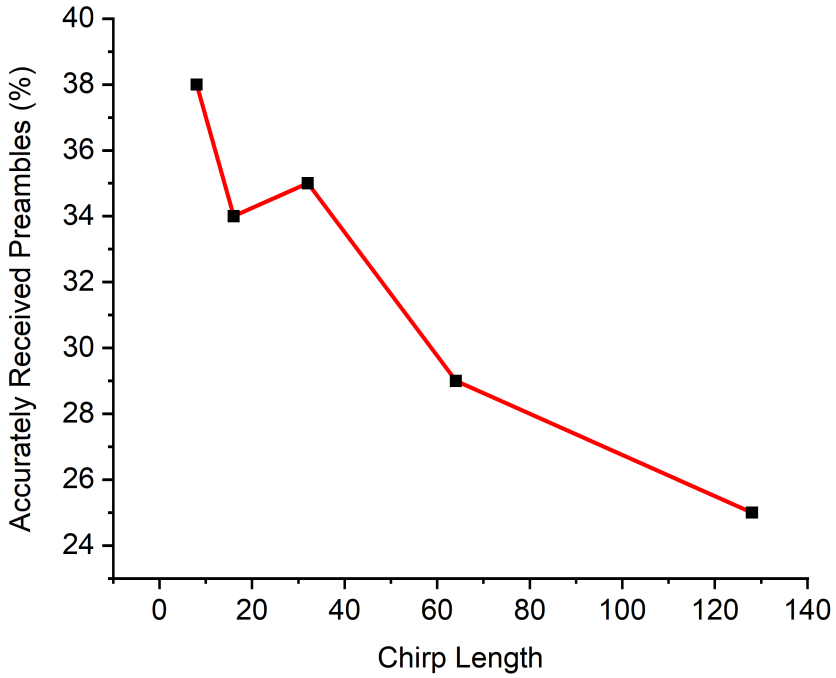


Fig. 5.4: Packet error rate for gold code modulation of various chip lengths

rate can be increased.

6 CONCLUSION

I proposed, designed, and prototyped PACT, a scalable communication algorithm that improves the communication range of battery-less Tags. Our Tag design using active radio avoids the range limitation due to dual path loss in existing passive backscatter systems. Our energy harvesting circuit design along with ultra-low power wake-up receiver and demodulator reduces the energy consumption of the Tag. Our Q&A-based communication paradigm where the Source queries the Tag with a specific Question further simplifies the Tag design and hence its energy consumption. Our hybrid MAC protocol allows more than 500 Tags to communicate concurrently with the Reader. We identify three key applications in food safety, transportation, and storage where PACT can be integrated. It can offer low-cost or no-cost monitoring and tracking options for these large-scale deployments over a long time, making PACT scalable and sustainable.

I proposed WiChronos, a modulation technique that enables long-range communication in large-scale deployments of energy-constrained sensor nodes. By offloading the communication complexity to timers present in every MCU, we reduce the energy consumption and the cost of each sender. We reduce the time-on-air by minimizing the number of symbols per message, in turn improving the spectral efficiency. The reduced time-on-air enables an ALOHA-based MAC protocol to accommodate a large-scale network without significantly affecting collision performance. We propose error detection and correction mechanisms for timing-induced bit errors for bounded errors. Using off-the-shelf RF modules and MCUs, I prototype and evaluated the energy, range, and scale performance experimentally in indoor and outdoor scenarios.

I present SatConnect, a continent-scale IoT technology that leverages pre-existing constellations of amateur radio satellites known as OSCARs to enable connectivity. SatConnect tags use CSS modulation at low transmit

power so that the payload is imperceptible to the human ear and appears as white noise. I will demonstrate experimentally that a SatConnect tag is capable of transmitting to a receiver located 1100km away.

Finally, I also worked on the design of link layer protocols in molecular communication networks. Embedding the device address in the signal amplitude and offloading the timer required to keep a count of the communication reduce the number of signals transmitted. This reduces the collision probability in a multi-sender network and maximizes the network throughput.

7 DISCUSSION

In this chapter, I present avenues towards my doctoral research can be extended further. The three systems I have built can not only be improved further, but they also be used in several other applications for alternate uses without any additional changes to the described hardware.

7.1 Future work for PACT

7.1.1 Alternate harvesting sources

It is possible to harvest energy from other sources to charge the storage capacitor faster [217], often leveraging the applications. For example, solar cells or piezoelectric crystals could be incorporated to the RF energy harvesting unit on the Tag. Most on-body applications could take advantage of piezoelectric crystals to harvest usable energy [218], and outdoor applications could use solar cells similar to pLoRa [12], or polymer triboelectric nanogenerators that convert mechanical to electrical energy.

7.1.2 Soil moisture detection using PACT tag

Though we present PACT in the context of monitoring applications, the PACT tag can be used with minimal to no changes for several other applications as well.

In Chapter 3, I explain the design and implementation of the prototype of a passive tag with an active radio that is able to achieve better communication range. Instead of increasing the communication range, the tags could be used to transmit across a medium that has a higher inherent path loss, and unlike backscatter, we'd still be able to receive the signals at the Reader. With this insight, we propose using the PACT tag to enable wireless moisture detection and estimation. Moisture detection required the

tags to be buried under the ground. The path loss of RF signals through moisture-laden soil is larger than dry soil or air. While the RSSI of a signal from a backscatter tag may not suffice, initial experiments indicate that it is possible to receive data with over 3dB SNR from a PACT tag buried underground in the presence of moist soil. We are exploring techniques to use the phase of the received signal to estimate the moisture content in the soil. Since a PACT tag is batteryless, it requires minimal maintenance. A drone carrying the source and reader can easily charge the tags as well as gather the tag responses. This data can be transferred to the cloud for additional computing to estimate the soil moisture. In the context of this application, PACT enables the vision of deploying sensor nodes on an extremely large scale without having to worry about the environmental footprint. Several techniques exist to build circuits on biodegradable PCBs. Since a PACT tag doesn't require a battery, there is potential to develop tags that are completely biodegradable.

7.1.3 Localization using PACT tag

Another possible use of the PACT tag is in the localization of devices in a closed/bounded indoor environment. We base this on the insight that the energy harvesting circuit on the tag charges to a voltage that is a function of the source signal power, the efficiency of the harvester, and the distance between the source and the tag. The harvester efficiency is hardware dependent but is consistent for a given PCB. If we keep the source power consistent, the voltage our RF harvester charges to is completely dependent on the distance from the excitation source. We propose to attach the source to the device that needs to be localized. The space where the source needs to be localized has several PACT tags in fixed locations across all the boundaries. By measuring the voltage across the storage capacitor on these tags, we can estimate the location of the source, and by extension, the device that needs to be localized. Before an algorithm

can be implemented, studies need to be done to determine the minimum sensitivity that is possible. The sensitivity could be better at frequencies other than the 915MHz band, though experimental verification is required for this. The harvester on the tag will work at all frequencies but will need the inductor and capacitor values on the matching circuit to be adjusted depending on the frequency chosen.

7.2 Future work for WiChronos

WiChronos is the first step towards a low-power, long-range, scalable wireless network for low data-rate LPWANs. There are open research challenges that need further investigation and new research areas stemming from our work, some of which are discussed here.

7.2.1 Timing error detection and correction

Existing error correction codes are designed for bit errors. Timing errors in WiChronos can occur due to distance, and channel conditions. Currently, we transmit anchor symbols at low data rates of the order of a few kbps, and hence the impact of the above conditions on anchor symbol timing is minimal. Error correction mechanisms will be needed for higher anchor symbol rates of 100s of kbps. We proposed a simple error correction mechanism for clock skew that uses the apriori knowledge of clock tolerance. Smarter, capacity achieving timing error correction can improve the data-rate performance of WiChronos, making it suitable for a wider range of applications.

7.2.2 Data-rate energy tradeoff

WiChronos trades off data rate for energy efficiency. We proposed two strategies to improve the data-rate performance of WiChronos. 1)A greedy

algorithm that uses prior knowledge of the source distribution. 2)Information-theoretic and machine learning approaches to learn the source distribution and encode data to clock cycles optimally; also an ongoing work. Systems research on efficient low-power, high-accuracy clocks have the potential to maximize data rate and minimize energy further.

7.2.3 Information security and authentication

In its current design, a WiChronos receiver identifies the sender from the anchor symbols and does not offer a mechanism for authentication. An adversary could be listening to the channel to decode data and it is therefore not secure. Encrypting anchor symbol bit pattern can be used to authenticate the sender whereas data security can be achieved by encrypting the data (D) to timing (T_{info})mapping. Simple and efficient security protocols for timing-based communication is a branch of research that is open for further study.

7.2.4 Physical layer

WiChronos was implemented using OTS components and we rely on their built-in signal processing for modulation and demodulation, frequency spectrum, and AGC timing among other features. Various other transceivers such as TI CC1101 and TI CC1125 offer advantages such as lower AGC settling time, the ability to detect a 4-bit preamble, and a much lower active current. Parameters for choosing appropriate hardware may be restricted by the application and requires further study. We are currently working on exploring some of these modules from TI.

7.3 Future work for Satellite IoT

In my work, I discuss the bit error rate results when using a gold code sequence as the modulation. We see that at low SNR, using the gold code results in higher errors and hence, a large number of packet losses. For better noise resilience and accurate demodulation and detection, CSS-based data modulation is proposed. Experiments using chirps of modulation order 16, 32, and 64 have shown promising results, though these have been conducted with the transmitter and ground station receiver co-located. The next step towards the implementation of the system is to verify the functionality of these devices at long ranges of 1000s of km and evaluate the bit error rate. With that in place, the next step towards a practical Satellite IoT system would require a deployment where multiple devices would be scheduled to transmit to the same satellite. Algorithms to resolve packet collisions and retrieve data from concurrently transmitted packets could increase the system scale. The accuracy of these algorithms shall be evaluated by measuring the bit error rate across the entire deployment. Experimental verification of the maximum achievable per node and system data rate shall be explored through the deployment. Several methods can be adopted to improve the data rate further. Allowing the capability to transmit to multiple satellites on each node is an example of such an extension to this work. Each node may be programmed to be sensitive to several beacon frequencies. This approach will increase the spectrum usage and hence, result in more collisions as well. A practical deployment will enable a better understanding of the number of satellites each node may have access to for best data rates versus for best network scale. Finally, further experimental verification is required to accurately understand the effect of scale on the audibility of the signal. The current user study only had one interfering data transmission going on in the background. A scaled deployment will be required to evaluate the upper bound on the node transmit power such that the packets appear as white noise still, but

have enough signal power at the receiver to be demodulated and detected with accuracy.

7.4 Community centered computing

The goal of my research so far has been to make fundamental contributions toward increasing the communication range of wireless systems. These contributions, while solving urgent technical problems, have sometimes been disconnected from larger societal and global issues. I intend to bridge the gap between these innovations in wireless systems, and direct application in community-directed science and sensors/data enabling civic action. This pivot to community-centered approaches towards the application of computing to undo the effects of climate change represents a significant new body of work I must engage with and understand, including literature not traditionally taught in electrical and computer engineering around socio-technical systems, ethics, power, position, and practical skills around qualitative information gathering and analysis. Further, by working with marginalized communities, such as Indigenous and Native American tribes, I must increase my understanding of governance and political science structures that inform and necessarily situate the work. No longer can I build things in a lab, but I must now co-design and invent for a purpose. This requires developing a fundamental and respectful understanding of the traditional ecological knowledge, systems, and co-production that has been preserved by these communities. Through close collaborations with the community members, I intend to create methodologies that combine state-of-the-art environmental sensing and data science with traditional land use ideologies to identify and evaluate potential solutions. My proposed ideas also pivot toward collaboration with bioengineers, specifically those involved with bacterial genetic engineering. I plan to use Microbial Fuel Cells for power generation and as sensors. Sensing using MFCs re-

quires the identification of bacteria that are sensitive to particular elements (carbon and nitrogen). Bacteria must be engineered so that pathways responsible for interactions of the bacteria with these elements can be amplified to enhance the accuracy of measurement. The combined learning and skill building from these two interconnected fields will greatly benefit my future as a scientist who hopes to build cutting-edge, yet practical and well situation technologies for combatting climate degradation on behalf and with marginalized communities on the frontlines of climate adaptations.

Having built a skillset to build and deploy prototypes in my doctoral research, I now hope to pivot towards enabling community-driven computing. I believe that capturing observations from communities and using these to inform my goals as a researcher will bring benefits to these communities sooner since I can create custom solutions and build digital hardware toolkits concurrently to be used across the spectrum of users. Marginalized and rural communities today face a disproportionate impact of climate change and land development practices like mining, oil/gas pipelines, etc. Low-cost and low-burden solutions are required for these communities to enable access to technology to understand, evaluate, and address the effects of climate change.

According to some estimates, native communities own only 2.6% of the total landmass of the United States. The increasing frequency of extreme weather events, the global rise in temperatures, and several human practices deter the ability of these communities to access and maintain natural resources. For example, Manoomin, the Ojibwe term for wild rice, grows in coastal wetlands. Manoomin has been grown and sustained by the Ojibwe tribe and other communities for centuries and is viewed as essential to the distinct identity of the Ojibwe people. Manoomin represents a connection to the community since they are both dependent on each other for survival and therefore, the Ojibwe people consider it to be

their innate responsibility to care for and protect the lands essential to their cultural practices. Despite owning a small part of the land in this country, these are tribes that practice sustainability in everyday practices. In fact, indigenous communities all across the world have internalized the idea that if they exhaust all their resources, their future generations will have nothing to eat or anywhere to live. By collaborating with nature, they have an intimate relationship with all the natural resources and care deeply about the conservation and well-being of these resources.

Grounded in the importance of understanding these relationships of the communities with nature, I propose a novel approach towards preserving these natural resources while being respectful of the practices and beliefs they hold dear. Though we need technologies to sense and monitor the detrimental effects of climate change, it is imperative that these do not add further to land use infringement.

Conservation efforts require regular monitoring of several environmental factors such as temperatures, humidity and moisture content of soil, several nutrients to monitor soil health, the flow of natural water sources, etc. All of these require several sensors to be deployed. Measurement of soil health and moisture requires sensors to be buried in the soil. Wireless devices are required to transmit this sensor data. Further, power sources are required to supply energy to all of these components.

Inspired by the practices that the tribes follow, I think the technology and the lands where it is implemented depend on each other. To enable this synergy, the sensors placed in the environment must not have any detrimental effects on the land. The PCBs that these sensors are fabricated on can be made on biodegradable mediums. However, batteries used to power these sensors are not biodegradable and result in polluting the land with harmful chemicals. I seek alternative ways to power and use the sensors through the lands themselves. I propose a novel approach towards integrating this wireless and sensor system with power derived

from Microbial Fuel Cells (MFC) to reduce the environmental footprint of this additional technology on these lands.

In its very basic form, MFCs use microorganisms feeding on a substrate such as wastewater or lignocellulosic biomass (dry plant matter), etc. Microbes oxidize the substrate on the anodic compartment of the cell and release an electron that travels through an external circuit (thereby powering it) to the cathode compartment. The anode and cathode compartments are separated by a proton exchange membrane through which protons are induced to maintain charge balance. The output power produced by MFCs depends on several factors such as the type of substrate, microorganisms, material for cathode and anode terminals, and circuit resistance. However, the greatest challenge in integrating MFCs with wireless circuits is that the power delivered by the MFCs is dynamic and depends on the environment. Rains and floods may raise the voltage by providing ideal growing conditions for the microorganisms. On the other hand, warmer days and summer months will need regular care to keep the MFCs up and functional. The type of soil varies from location to location. Different types of soil impact the growth of bacteria and hence change the total power that can be produced. Since power production is not guaranteed to be regular, sudden power failures are bound to happen. The state of the system at different points must be maintained and stored so that measured data is not lost when this happens. Therefore, the sensing and data transfer hardware as well as software protocol designed around these systems must be able to navigate these challenges.

I propose further exploration with MFCs in using them as the sensors for soil health as well as the power source for data transfer. MFCs have been shown to successfully remove carbon and nitrogen from wastewater by up to 50%. Looking at it from a different perspective, I would claim that MFCs can detect the presence of carbon and nitrogen and the power output is sensitive to the concentration of carbon and nitrogen. Therefore,

the power output produced by the MFC is an indication of the Carbon and Nitrogen levels in the soil. A practical deployment of such a sensor will consist of several cells with varying densities of microorganisms. I propose algorithms to eliminate errors due to the differences in microorganism concentration by following the principles of differential noise cancellation (which is used in several digital and analog circuits).

Once the sensors have measured the required data, I propose using backscatter communication for data transfer. Much research on backscatter has already positioned it as one of the most commonly used low-power communication models for battery-free devices.

In summary, my work provides solutions towards achieving a long communication range, much research effort needs to be dedicated to deploying these devices and studying the long-term effects so that these could eventually be converted into products that can enhance the quality of human life.

BIBLIOGRAPHY

[1] Smart Animal Production. https://lora-alliance.org/wp-content/uploads/2020/12/THE-FARMING-OF-TOMORROW-IS-ALREADY-HERE-HOW-LoRaWAN%C2%AE-TECHNOLOGY-SUPPORTS-SMART-AGRICULTURE-PRECISE-ANIMAL//-PRODUCTION.pdf.

[2] Precision Agriculture. https://cdn2.hubspot.net/hubfs/2507363/Semtech_Smart_Agriculture_White_Paper.pdf.

[3] Smart Building. https://lora-alliance.org/wp-content/uploads/2020/11/LA_WhitePaper_SmartBuildings_0520_v1.1_1.pdf.

[4] Smart Planet. https://info.semtech.com/hubfs/Semtech-UseCase-EBook-SmartPlanet_locked.pdf?hsCtaTracking=a1c4b6e2-c4a4-4fa6-942f-639ad15a6518%7C769d05d8-4178-4854-8ee6-f34d756fc141.

[5] IoT Statistics. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

[6] State of IoT 2023. https://iot-analytics.com/number-connected-iot-devices/.

[7] 80+ Amazing IoT Statistics (2023-2030). https://explodingtopics.com/blog/iot-stats.

[8] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R Smith. Ambient backscatter: wireless communication out of thin air. In *ACM SIGCOMM Computer Communication Review*, volume 43, pages 39–50. ACM, 2013.

[9] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3):1–24, 2017.

[10] Anran Wang, Vikram Iyer, Vamsi Talla, Joshua R Smith, and Shyamnath Gollakota. {FM} backscatter: Enabling connected cities and smart fabrics. In *14th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 17)*, pages 243–258, 2017.

[11] Mohammad Rostami, Karthik Sundaresan, Eugene Chai, Sampath Rangarajan, and Deepak Ganesan. Redefining passive in backscattering with commodity devices. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, MobiCom '20, New York, NY, USA, 2020. Association for Computing Machinery.

[12] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. Plora: A passive long-range data network from ambient lora transmissions. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*. ACM, 2018.

[13] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3):105, 2017.

[14] Mohammad Rostami, Karthik Sundaresan, Eugene Chai, Sampath Rangarajan, and Deepak Ganesan. Redefining passive in backscattering with commodity devices. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, MobiCom '20, New York, NY, USA, 2020. Association for Computing Machinery.

[15] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R Smith, and David Wetherall. Wi-fi backscatter: Internet connectivity for rf-powered devices. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, pages 607–618, 2014.

[16] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R Smith. Ambient backscatter: Wireless communication out of thin air. *ACM SIGCOMM Computer Communication Review*, 43(4):39–50, 2013.

[17] Daniel J Yeager, Alanson P Sample, Joshua R Smith, and Joshua R Smith. Wisp: A passively powered uhf rfid tag with sensing and computation. *RFID handbook: Applications, technology, security, and privacy*, pages 261–278, 2008.

[18] Passive RFID Tag. https://www.aliexpress.com/item/2255800522580150.html?spm=a2g0o.ppclist.product.2.641bE6GBE6GBWs&pdp_npi=2%40dis%21USD%21US%20%240.12%21US%20%240.12%21%21%21%21%21%402101f6b716605809052758111e8b23%2110000006217488383%21btf&_t=pvid:0f17c373-4fc3-4318-8015-63088b7ccfc5&afTraceInfo=4000708894902__pc__pcBridgePPC__xxxxxx__1660580905.

[19] M. S. Trotter and G. D. Durgin. Survey of range improvement of commercial rfid tags with power optimized waveforms. In *2010 IEEE International Conference on RFID (IEEE RFID 2010)*, pages 195–202. IEEE, 2010.

[20] Deepak Ganesan Pan Hu, Pengyu Zhang. Laissez-faire : Fully asymmetric backscatter communication. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, pages 255–267. ACM, 2015.

[21] Gen2 passive RFID tags from SkyRFID. https://skyrfid.com/RFID_Range.php.

[22] Matti Siekkinen, Markus Hiienkari, Jukka K Nurminen, and Johanna Nieminen. How low energy is bluetooth low energy? comparative measurements with zigbee/802.15. 4. In *2012 IEEE wireless communications and networking conference workshops (WCNCW)*, pages 232–237. IEEE, 2012.

[23] J. F. Ensworth and M. S. Reynolds. Ble-backscatter: Ultralow-power iot nodes compatible with bluetooth 4.0 low energy (ble) smartphones and tablets. *IEEE Transactions on Microwave Theory and Techniques*, 65(9):3360–3368, 2017.

[24] LoRa. https://www.semtech.com/lora.

[25] Jothi Prasanna Shanmuga Sundaram, Wan Du, and Zhiwei Zhao. A survey on lora networking: Research problems, current solutions and open issues, 2019.

[26] SigFox. https://www.sigfox.com/en/sigfox-iot-radio-technology.

[27] NB-IoT. https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/.

[28] Shahin Farahani. *ZigBee wireless networks and transceivers*. Newnes, 2011.

[29] Lacuna. https://lacuna.space/about/.

[30] Swarm. https://swarm.space/applications/.

[31] Starlink. https://starlink.com/.

[32] Zebra FX9600 RFID Reader. https://www.atlasrfidstore.com/zebra-fx9600-rfid-reader-4-port/.

[33] Zebra MC3330 XR RFID Reader. https://www.atlasrfidstore.com/zebra-mc3330xr-integrated-rfid-handheld-reader/.

[34] Po-Han Peter Wang, Haowei Jiang, Li Gao, Pinar Sen, Young-Han Kim, Gabriel M Rebeiz, Patrick P Mercier, and Drew A Hall. A 6.1-nw wake-up receiver achieving- 80.5-dbm sensitivity via a passive pseudo-balun envelope detector. *IEEE Solid-State Circuits Letters*, 1(5):134–137, 2018.

[35] Jesse Moody, Pouyan Bassirian, Abhishek Roy, Yukang Feng, Shuo Li, Robert Costanzo, N Scott Barker, Benton Calhoun, and Steven M Bowers. An 8.3 nw- 72 dbm event driven ioe wake up receiver rf front end. In *2017 12th European Microwave Integrated Circuits Conference (EuMIC)*, pages 77–80. IEEE, 2017.

[36] Travis L Cochran, Jeong Ki Kim, and Dong Sam Ha. Low power wake-up receiver with unique node addressing. In *2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 1–4. IEEE, 2011.

[37] P Woias, S Heller, and U Pelz. A highly sensitive and ultra-low-power wake-up receiver for energy-autonomous embedded systems. *JPhCS*, 1052(1):012024, 2018.

[38] Efento IoT platform for sensor data in the cloud. https://getefento.com/technology/efento-cloud-an-iot-platform-for-sensor-data/.

[39] Monnit. https://www.monnit.com/applications/food-service-monitoring/.

[40] Icicle : Food production software. https://icicletechnologies.com/2018/03/12/icicle-and-bell-partner-bring-unique-iot-\solutions-canadas-food-industry/.

[41] iFoodDS. https://www.ifoodds.com/.

[42] Varcode:Affordable Digital Collection, Recording, Tracing and Reporting for Supply Chain Compliance . https://www.varcode.com/.

[43] ZestLabs : Freshness Management. https://www.zestlabs.com/.

[44] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. Hitchhike: Practical backscatter using commodity wifi. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, SenSys '16, page 259–271, New York, NY, USA, 2016. Association for Computing Machinery.

[45] Luca Feltrin, Chiara Buratti, Enrico Vinciarelli, Roberto De Bonis, and Roberto Verdone. Lorawan: Evaluation of link-and system-level performance. *IEEE Internet of Things Journal*, 5(3):2249–2258, 2018.

[46] Saman Naderiparizi, Aaron N. Parks, Zerina Kapetanovic, Benjamin Ransford, and Joshua R. Smith. Wispcam: A battery-free rfid camera. In *2015 IEEE International Conference on RFID (RFID)*, pages 166–173, 2015.

[47] Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua R. Smith. Battery-free cellphone. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(2), jun 2017.

[48] Zigbee 3.0. https://www.nxp.com/products/wireless/zigbee/zigbee/zigbee-3.0:ZIGBEE-3-0.

[49] How Cell Towers Work to Keep You Connected. https://www.ni.com/en/solutions/semiconductor/wireless-infrastructure-development/how-cell-towers-work.html.

[50] Cell Tower Range. https://dgtlinfra.com/cell-tower-range-how-far-reach/.

[51] Temperature Control and Food Safety Software: An Evolving Discipline. https://globalfoodsafetyresource.com/temperature-control-and-food-safety-software-three-\options-for-success/.

[52] Transportation can be tricky for dairy processors. https://www.dairyfoods.com/articles/95019-transportation-can-be-tricky-for-dairy-processors.

[53] Jenny Gustavsson, Christel Cederberg, Ulf Sonesson, Robert van Otterdijk, and Alexandre Meybeck. Global food losses and food waste: extent, causes and prevention. 2011.

[54] Sonesson U Otterdijk Rv Meybeck A Gustavsson J, Cederberg C. Global food losses and food waste: extent, causes and prevention, 2011.

[55] Perishable goods transportation market. https://www.prnewswire.com/news-releases/perishable-goods-transportation-market-to-register-a-\growth-of-usd-6-43-billion-at-a-cagr-of-7-22--rising-\demand-for-processed-food-is-a-key-driver-\-technavio-301527222.html.

[56] FDA Seeks Innovative Food Traceability Tools on Advancing Food Safety with Technology. https://www.fda.gov/news-events/fda-voices/fda-seeks-innovative-food-traceability-tools-and-opens-\dialogue-advancing-food-safety-technology.

[57] New Era of Smarter Food Safety Blueprint. https://www.fda.gov/food/new-era-smarter-food-safety/new-era-smarter-food-safety-blueprint.

[58] The State of Food and Agriculture Report. https://www.fao.org/publications/sofa/2019/en/.

[59] Time/Temperature for Safety. https://blog.smartsense.co/time-temp-control-food-safety.

[60] G. A. Casula, G. Montisci, A. Michel, and P. Nepa. Analysis of wearable ungrounded antennas for uhf rfids with respect to the coupling with human-body. In *2016 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, pages 6–9, 2016.

[61] V. Talla, S. Pellerano, H. Xu, A. Ravi, and Y. Palaskas. Wi-fi rf energy harvesting for battery-free wearable radio platforms. In *2015 IEEE International Conference on RFID (RFID)*, pages 47–54, 2015.

[62] Bibin Varghese, Nidhin Easow John, S. Sreelal, and Karthika Gopal. Design and development of an rf energy harvesting wireless sensor node (eh-wsn) for aerospace applications. *Procedia Computer Science*, 93:230–237, 2016. Proceedings of the 6th International Conference on Advances in Computing and Communications.

[63] Hiroshi Nishimoto, Yoshihiro Kawahara, and Tohru Asami. Prototype implementation of ambient rf energy harvesting wireless sensor networks. In *SENSORS, 2010 IEEE*, pages 1282–1287, 2010.

[64] Thien D. Nguyen, Jamil Y. Khan, and Duy T. Ngo. An adaptive mac protocol for rf energy harvesting wireless sensor networks. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2016.

[65] Smartrac dogbone. https://rfid.averydennison.com/en/home/product-finder/sensor-dogbone.html.

[66] Eiichiro Fujiwara and Masaru Aoki. Rectenna, December 5 2017. US Patent 9,837,857.

[67] Ambuj Varshney, Oliver Harms, Carlos Pérez-Penichet, Christian Rohner, Frederik Hermans, and Thiemo Voigt. Lorea: A backscatter architecture that achieves a long communication range. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, pages 1–14, 2017.

[68] Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Ahmad Siddiqi, and Yunhao Liu. Aloba: rethinking on-off keying modulation for ambient lora backscatter. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, pages 192–204, 2020.

[69] Gordon L Stüber and Gordon L Steuber. *Principles of mobile communication*, volume 2. Springer, 1996.

[70] AMIHUD KRAMER. "Effect of storage on nutritive value of food 1". *Journal of food quality*, 1(1):23–55, 1977.

[71] Sean T. Hammond, James H. Brown, Joseph R. Burger, Tatiana P. Flanagan, Trevor S. Fristoe, Norman Mercado-Silva, Jeffrey C. Nekola, and Jordan G. Okie. Food Spoilage, Storage, and Transport: Implications for a Sustainable Future. *BioScience*, 65(8):758–768, 06 2015.

[72] Cold preservation of meat products. https://www.fao.org/3/T0098E/T0098E02.htm.

[73] STEPHEN G Campano and PARKER W Hall Jr. Time and temperature controls. In *Proceedings of the 50th Annual Reciprocal Meat Conference, Iowa State University, Ames, Iowa, Jun*, pages 25–32.

[74] Marco Baldi and E. Gambi. *MAC Protocols for RFID Systems*. 02 2010.

[75] Ibrahim Amadou, Abdoul Aziz Mbacké, and Nathalie Mitton. How to improve csma-based mac protocol for dense rfid reader-to-reader networks? In Song Guo, Jaime Lloret, Pietro Manzoni, and Stefan Ruehrup, editors, *Ad-hoc, Mobile, and Wireless Networks*, pages 183–196, Cham, 2014. Springer International Publishing.

[76] Anonymized GitHub repository. `https://anonymous.4open.science/r/PACT`.

[77] TI CC1125 datasheet. `http://www.ti.com/lit/ds/symlink/cc1125.pdf`.

[78] MSP 430 FR2355. `http://www.ti.com/product/MSP430FR2353`.

[79] Tagsense active tag. `https://rfidstore.myshopify.com/products/usb-active-rfid-kit`.

[80] Joshua F Ensworth and Matthew S Reynolds. Ble-backscatter: Ultralow-power iot nodes compatible with bluetooth 4.0 low energy (ble) smartphones and tablets. *IEEE Transactions on Microwave Theory and Techniques*, 65(9):3360–3368, 2017.

[81] SMS7630-040LF. `https://store.skyworksinc.com/products/detail/sms7630-040lf-skyworks-solutions-inc/418268/`.

[82] Ncs2200sq2t2g.

[83] Ax5043 low-power radio.

[84] Masaki Muramatsu and Hirotaka Koizumi. An experimental result using rf energy harvesting circuit with dickson charge pump. In *2010 IEEE International Conference on Sustainable Energy Technologies (ICSET)*, pages 1–4. IEEE, 2010.

[85] Blake R Marshall, Marcin M Morys, and Gregory D Durgin. Parametric analysis and design guidelines of rf-to-dc dickson charge pumps for rfid energy harvesting. In *2015 IEEE International Conference on RFID (RFID)*, pages 32–39. IEEE, 2015.

[86] Nathan E Roberts and David D Wentzloff. A 98nw wake-up radio for wireless body area networks. In *2012 IEEE Radio Frequency Integrated Circuits Symposium*, pages 373–376. IEEE, 2012.

[87] K Kaushik, Deepak Mishra, Swades De, Kaushik Roy Chowdhury, and Wendi Heinzelman. Low-cost wake-up receiver for rf energy harvesting wireless sensor networks. *IEEE Sensors Journal*, 16(16):6270–6278, 2016.

[88] Po-Han Peter Wang, Haowei Jiang, Li Gao, Pinar Sen, Young-Han Kim, Gabriel M Rebeiz, Patrick P Mercier, and Drew A Hall. A near-zero-power wake-up receiver achieving- 69-dbm sensitivity. *IEEE Journal of Solid-State Circuits*, 53(6):1640–1652, 2018.

[89] Tinyfpga ax & bx.

[90] Sinem Coleri Ergen and Pravin Varaiya. Tdma scheduling algorithms for wireless sensor networks. *Wireless networks*, 16(4):985–997, 2010.

[91] Shailesh M Birari and Sridhar Iyer. Mitigating the reader collision problem in rfid networks with mobile readers. In *2005 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf on Communic*, volume 1, pages 6–pp. IEEE, 2005.

[92] M. Ghovanloo and K. Najafi. A wideband frequency-shift keying wireless link for inductively powered biomedical implants. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 51(12):2374–2383, 2004.

[93] ZHL 42W. `https://www.minicircuits.com/WebStore/dashboard.html?model=ZHL-42W%2B`.

[94] HitchHike GitHub. `https://github.com/pengyuzhang/HitchHike`.

[95] R. van Langevelde, M. van Elzakker, D. van Goor, H. Termeer, J. Moss, and A. J. Davie. An ultra-low-power 868/915 mhz rf transceiver for wireless sensor network applications. In *2009 IEEE Radio Frequency Integrated Circuits Symposium*, pages 113–116, 2009.

[96] Moein Khazraee, Yeswanth Guddeti, Sam Crow, Alex C Snoeren, Kirill Levchenko, Dinesh Bharadia, and Aaron Schulman. Sparsdr: Sparsity-proportional backhaul and compute for sdrs. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, pages 391–403, 2019.

[97] Revathy Narayanan, Swarun Kumar, and Siva Ram Murthy. Cross technology distributed mimo for low power iot. *IEEE Transactions on Mobile Computing*, 2020.

[98] Nikolaus Kleber, Jonathan Chisum, Aaron Striegel, Bertrand Hochwald, Abbas Termos, J Nicholas Laneman, Zuohui Fu, and John Merritt. Radiohound: A pervasive sensing network for sub-6 ghz dynamic spectrum monitoring. *arXiv preprint arXiv:1610.06212*, 2016.

[99] TinyFPGA nano. `https://www.aliexpress.com/item/3256801887502111.html?gatewayAdapt=4itemAdapt`.

[100] MESA 5123. `http://store.mesanet.com/index.php?route=product/product&product_id=65`.

[101] USRP B200. `https://www.ettus.com/all-products/ub200-kit/`.

[102] USRP B200. `https://www.amazon.com/RTL-SDR-Blog-RTL2832U-Software-Defined/dp/B0129EBDS2`.

[103] Siva Racer. `https://www.atlasrfidstore.com/siva-custom-foam-backed-racer-rfid-tag-nxp-ucode-8/`.

[104] Winners of fda's low- or no-cost food traceability challenge. `https://www.fda.gov/food/new-era-smarter-food-safety/meet-winners-fdas-low-or-no-cost-food-traceability-\challenge`.

[105] FDA Blueprint for the Future. `https://www.fda.gov/media/139868/download`.

[106] Food Storage. `https://food.unl.edu/article/refrigerator-and-freezer-storage`.

[107] Drug Supply Chain Security Act (DSCSA). https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa.

[108] Cold Chain Monitoring. https://www.monnit.com/applications/cold-chain-monitoring/.

[109] Transport of medicines and vaccines. https://getefento.com/application/transport-of-medicines-and-vaccines/.

[110] Proper storage of medicines in pharmacies . https://getefento.com/application/proper-storage-of-medicines-in-pharmacies/.

[111] FDA Blueprint for the Future. https://www.unep.org/news-and-stories/story/why-optimized-cold-chains-could-save-\billion-covid-vaccines.

[112] FDA Blueprint for the Future. https://theconversation.com/cracking-the-cold-chain-challenge-is-key-to-\making-vaccines-ubiquitous-99329.

[113] Bing Dong, Vishnu Prakash, Fan Feng, and Zheng O'Neill. A review of smart building sensing system for better indoor environment control. *Energy and Buildings*, 199:29–46, 2019.

[114] Corporate Property Remote Monitoring Applications. https://monnit.blob.core.windows.net/site/documents/whitepapers/MWP007-Corporate-Facilities-Whitepaper.pdf.

[115] Leveraging the Internet of Things for Competitive Advantage. https://knowledge.wharton.upenn.edu/article/leveraging-the-internet-of-things-for\-competitive-advantage/.

[116] GreenHouse Monitoring. https://www.monnit.com/applications/greenhouse-monitoring/.

[117] Remote Monitoring Solutions for Data Centers and Server Rooms . https://www.monnit.com/applications/data-center-server-room-monitoring.

[118] Aaron N. Parks, Alanson P. Sample, Yi Zhao, and Joshua R. Smith. A wireless sensing platform utilizing ambient rf energy. In *2013 IEEE Topical Conference on Biomedical Wireless Technologies, Networks, and Sensing Systems*, pages 154–156, 2013.

[119] Jingxian Liu, Ke Xiong, Pingyi Fan, and Zhangdui Zhong. Rf energy harvesting wireless powered sensor networks for smart cities. *IEEE Access*, 5:9348–9358, 2017.

[120] Li Chen, Jeremy Warner, Pak Lam Yung, Dawei Zhou, Wendi Heinzelman, Ilker Demirkol, Ufuk Muncuk, Kaushik Chowdhury, and Stefano Basagni. Reach2-mote: A range-extending passive wake-up wireless sensor node. *ACM Transactions on Sensor Networks (TOSN)*, 11(4):1–33, 2015.

[121] Johannes Blobel, Vu Huy Tran, Archan Misra, and Falko Dressler. Low-power downlink for the internet of things using ieee 802.11-compliant wake-up receivers. In *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, pages 1–10, 2021.

[122] Joshua R. Smith, Bing Jiang, Sumit Roy, Matthai Philipose, Kishore Sundara-Rajan, and Alexander V. Mamishev. Id modulation: Embedding sensor data in an rfid timeseries. In *Information Hiding*, 2005.

[123] Tengxiang Zhang, Nicholas Becker, Yuntao Wang, Yuan Zhou, and Yuanchun Shi. Bitid: Easily add battery-free wireless sensors to everyday objects. In *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 1–8, 2017.

[124] Micah Adler and Bruce M Maggs. Protocols for asymmetric communication channels. *Journal of Computer and System Sciences*, 63(4):573–596, 2001.

[125] John Watkinson. *New protocols for asymmetric communication channels*. PhD thesis, National Library of Canada= Bibliothèque nationale du Canada, 2001.

[126] Mare Srbinovska, Cvetan Gavrovski, Vladimir Dimcev, Aleksandra Krkoleva, and Vesna Borozan. Environmental parameters monitoring in precision agriculture using wireless sensor networks. *Journal of cleaner production*, 88:297–307, 2015.

[127] JA López Riquelme, Fulgencio Soto, J Suardíaz, P Sánchez, Andres Iborra, and JA Vera. Wireless sensor networks for precision horticulture in southern spain. *Computers and electronics in agriculture*, 68(1):25–35, 2009.

[128] Hanwook Chung, Jingjie Li, Younghyun Kim, and Christopher Y Choi. Continuous and wireless skin contact and ear implant temperature measurements and relations to the core body temperature of heat stressed dairy cows. In *10th International Livestock Environment Symposium (ILES X)*, page 1. American Society of Agricultural and Biological Engineers, 2018.

[129] Haider Jawad, Rosdiadee Nordin, Sadik Gharghan, Aqeel Jawad, and Mahamod Ismail. Energy-efficient wireless sensor networks for precision agriculture: A review. *Sensors*, 17(8):1781, 2017.

[130] National Soil Moisture Network. `http://nationalsoilmoisture.com/`.

[131] National Ecological Observatory Network. `https://www.neonscience.org/`.

[132] Decagon 10HS Soil Moisture Sensor. `http://www.labcell.com/environmental/soil-moisture-sensors/10hs-soil-moisture-sensor`.

[133] EC5 Soil Moisture Sensor. `http://www.labcell.com/environmental/soil-moisture-sensors/ec5-soil-moisture-sensor`.

[134] TEROS 12: Avanced soil moisture sensing. `https://www.metergroup.com/environment/products/teros-12/`.

[135] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors*, 12(9):11734–11753, 2012.

[136] Colby Boyer and Sumit Roy. —invited paper—backscatter communication and rfid: Coding, energy, and mimo analysis. *IEEE Transactions on Communications*, 62(3):770–785, 2014.

[137] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[138] V. Pillai, H. Heinrich, D. Dieska, P. V. Nikitin, R. Martinez, and K. V. S. Rao. An ultra-low-power long range battery/passive rfid tag for uhf and microwave bands with a current consumption of 700 na at 1.5 v. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 54(7):1500–1512, 2007.

[139] Juha Petäjäjärvi, Konstantin Mikhaylov, Matti Hämäläinen, and Jari Iinatti. Evaluation of lora lpwan technology for remote health and wellbeing monitoring. In *2016 10th International Symposium on Medical Information and Communication Technology (ISMICT)*, pages 1–5. IEEE, 2016.

[140] Ruslan Kirichek and Vyacheslav Kulik. Long-range data transmission on flying ubiquitous sensor networks by using lpwan protocols. In *International Conference on Distributed Computer and Communication Networks*. Springer, 2016.

[141] William Hart Hayt, John A Buck, et al. *Engineering electromagnetics*, volume 6. McGraw-Hill New York, 1981.

[142] MSP 430 user guide. `http://www.ti.com/lit/ug/slau445i/slau445i.pdf`.

[143] Linx NT Series Transceiver User Guide. `https://linxtechnologies.com/wp/wp-content/uploads/trm-fff-nt.pdf`.

[144] Gregory J Pottie and William J Kaiser. Wireless integrated network sensors. *Communications of the ACM*, 43(5):51–58, 2000.

[145] Vijay Raghunathan, Curt Schurgers, Sung Park, and Mani B Srivastava. Energy-aware wireless microsensor networks. *IEEE Signal processing magazine*, 2002.

[146] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, and Andrea Passarella. Energy conservation in wireless sensor networks: A survey. *Ad hoc networks*, 7(3):537–568, 2009.

[147] Tifenn Rault, Abdelmadjid Bouabdallah, and Yacine Challal. Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks*, 2014.

[148] Ridha Soua and Pascale Minet. A survey on energy efficient techniques in wireless sensor networks. In *2011 4th Joint IFIP Wireless and Mobile Networking Conference (WMNC 2011)*, pages 1–9. IEEE, 2011.

[149] Gang Lu, Bhaskar Krishnamachari, and Cauligi S Raghavendra. An adaptive energy-efficient and low-latency mac for data gathering in wireless sensor networks. In *18th International Parallel and Distributed Processing Symposium, 2004. Proceedings.*, page 224. IEEE, 2004.

[150] Ilker Demirkol, Cem Ersoy, and Fatih Alagoz. Mac protocols for wireless sensor networks: a survey. *IEEE Communications Magazine*, 44(4):115–121, 2006.

[151] Wei Ye, John Heidemann, and Deborah Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on Networking (ToN)*, 12(3):493–506, 2004.

[152] Andrea Goldsmith. *Wireless communications*. Cambridge university press, 2005.

[153] Injong Rhee, Ajit Warrier, Mahesh Aia, Jeongki Min, and Mihail L Sichitiu. Z-mac: a hybrid mac for wireless sensor networks. *IEEE/ACM Transactions on Networking (TON)*, 16(3):511–524, 2008.

[154] Naoto Kimura and Shahram Latifi. A survey on data compression in wireless sensor networks. In *International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II*, volume 2, pages 8–13. IEEE, 2005.

[155] David Chu, Amol Deshpande, Joseph M Hellerstein, and Wei Hong. Approximate data collection in sensor networks using probabilistic models. In *22nd International Conference on Data Engineering (ICDE'06)*, pages 48–48. IEEE, 2006.

[156] Bhargav Kanagal and Amol Deshpande. Online filtering, smoothing and probabilistic modeling of streaming data. In *2008 IEEE 24th International Conference on Data Engineering*, pages 1160–1169. IEEE, 2008.

[157] Aria Nosratinia, Todd E Hunter, and Ahmadreza Hedayat. Cooperative communication in wireless networks. *IEEE communications Magazine*, 2004.

[158] Zhong Zhou, Shengli Zhou, Shuguang Cui, and Jun-Hong Cui. Energy-efficient cooperative communication in a clustered wireless sensor network. *IEEE Transactions on Vehicular Technology*, 2008.

[159] Paolo Casari, Alessia Marcucci, Michele Nati, Chiara Petrioli, and Michele Zorzi. A detailed simulation study of geographic random forwarding (geraf) in wireless sensor networks. In *MILCOM 2005-2005 IEEE Military Communications Conference*, pages 59–68. IEEE, 2005.

[160] Jamal N Al-Karaki and Ahmed E Kamal. Routing techniques in wireless sensor networks: a survey. *IEEE wireless communications*, 11(6):6–28, 2004.

[161] Vamsi Paruchuri, Shivakumar Basavaraju, Arjan Durresi, Rajgopal Kannan, and S Sitharama Iyengar. Random asynchronous wakeup protocol for sensor networks. In *First International Conference on Broadband Networks*. IEEE, 2004.

[162] IEEE Standard 802.15.4. `https://standards.ieee.org/standard/802_15_8-2017.html`.

[163] Benjie Chen, Kyle Jamieson, Hari Balakrishnan, and Robert Morris. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. *Wireless networks*, 8(5):481–494, 2002.

[164] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routing protocols for mobile ad hoc networks. *Ad hoc networks*, 2(1):1–22, 2004.

[165] Vikram Iyer, Rajalakshmi Nandakumar, Anran Wang, Sawyer Fuller, and Shyamnath Gollakota. Living iot: A flying wireless platform on live insects. *arXiv preprint arXiv:1812.09419*, 2018.

[166] Evşen Yanmaz, Saeed Yahyanejad, Bernhard Rinner, Hermann Hellwagner, and Christian Bettstetter. Drone networks: Communications, coordination, and sensing. *Ad Hoc Networks*, 68:1–15, 2018.

[167] Rapeepat Ratasuk, Nitin Mangalvedhe, Yanji Zhang, Michel Robert, and Jussi-Pekka Koskinen. Overview of narrowband iot in lte rel-13. In *2016 IEEE conference on standards for communications and networking (CSCN)*, pages 1–7. IEEE, 2016.

[168] Venkat Anantharam and Sergio Verdu. Bits through queues. *IEEE Transactions on Information Theory*, 42(1):4–18, 1996.

[169] Anand S Bedekar and Murat Azizoglu. The information-theoretic capacity of discrete-time queues. *IEEE Transactions on Information Theory*, 1998.

[170] Rajesh Sundaresan and Sergio Verdú. Robust decoding for timing channels. *IEEE Transactions on information Theory*, 46(2):405–419, 2000.

[171] Rajesh Sundaresan and Sergio Verdú. Capacity of queues via point-process channels. *IEEE/ACM Transactions on Networking (TON)*, 14(SI):2697–2709, 2006.

[172] Balaji Prabhakar and Robert Gallager. Entropy and the timing capacity of discrete queues. *IEEE Transactions on Information Theory*, 49(2):357–370, 2003.

[173] Sarah H Sellke, C-C Wang, Saurabh Bagchi, and Ness Shroff. Tcp/ip timing channels: Theory to implementation. In *IEEE INFOCOM 2009*. IEEE, 2009.

[174] Pandurang Kamat, Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Temporal privacy in wireless sensor networks: Theory and practice. *ACM Transactions on Sensor Networks (TOSN)*, 5(4):28, 2009.

[175] Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Anti-jamming timing channels for wireless networks. In *Proceedings of the first ACM conference on Wireless network security*, pages 203–213. ACM, 2008.

[176] Yujie Zhu and Raghupathy Sivakumar. Challenges: communication through silence in wireless sensor networks. In *Proceedings of the 11th annual international conference on Mobile computing and networking*, pages 140–147. ACM, 2005.

[177] Da-shan Shiu and Joseph M Kahn. Differential pulse-position modulation for power-efficient optical communication. *IEEE transactions on communications*, 47(8):1201–1210, 1999.

[178] Zabih Ghassemlooy, AR Hayes, NL Seed, and ED Kaluarachchi. Digital pulse interval modulation for optical communications. *IEEE Communications Magazine*, 36(12):95–99, 1998.

[179] Hisayoshi Sugiyama and Kiyoshi Nosu. Mppm: A method for improving the band-utilization efficiency in optical ppm. *Journal of Lightwave Technology*, 7(3):465–472, 1989.

[180] Hyuncheol Park and J. R. Barry. Trellis-coded multiple-pulse-position modulation for wireless infrared communications. *IEEE Transactions on Communications*, 52(4):643–651, April 2004.

[181] Hyuncheol Park and J. R. Barry. Modulation analysis for wireless infrared communications. In *Proceedings IEEE International Conference on Communications ICC '95*, volume 2, pages 1182–1186 vol.2, June 1995.

[182] Li Zhao and A. M. Haimovich. Multi-user capacity of m-ary ppm ultra-wideband communications. In *2002 IEEE Conference on Ultra Wideband Systems and Technologies (IEEE Cat. No.02EX580)*, pages 175–179, May 2002.

[183] Li Zhao and A. M. Haimovich. Capacity of m-ary ppm ultra-wideband communications over awgn channels. In *IEEE Vehicular Technology Conference*, 2001.

[184] Zhi Zhang, Zhonghai Lu, Qiang Chen, Xiaolang Yan, and Li-Rong Zheng. Code division multiple access/pulse position modulation ultra-wideband radio frequency identification for internet of things: concept and analysis. *International Journal of Communication Systems*, 25(9):1103–1121, 2012.

[185] Francesca Cuomo and C Martello. Mac principles for an ultra wide band wireless access. In *IEEE Global Telecommunications Conference (Cat. No. 01CH37270)*, 2001.

[186] Xuemin Shen, Weihua Zhuang, Hai Jiang, and Jun Cai. Medium access control in ultra-wideband wireless networks. *IEEE Transactions on Vehicular Technology*, 54(5):1663–1677, 2005.

[187] Dong Sam Ha and Patrick R Schaumont. Replacing cryptography with ultra wideband modulation in secure rfid. In *2007 IEEE International Conference on RFID*.

[188] Z. Lin and P. Wei. Pulse position modulation time hopping ultra wideband sharing signal for radar and communication system. In *2006 CIE International Conference on Radar*, pages 1–4, Oct 2006.

[189] R. Scholtz. Multiple access with time-hopping impulse modulation. In *Proceedings of IEEE Military Communications Conference*, 1993.

[190] STM32L151x6. `https://www.st.com/resource/en/datasheet/cd00277537.pdf`.

[191] TI CC1101 datasheet. `www.ti.com/lit/gpn/cc1101`.

[192] Long-range RF communication:. `http://www.ti.com/lit/wp/swry006/swry006.pdf`.

[193] Matthew Gast. *802.11 wireless networks: the definitive guide*. " O'Reilly Media, Inc.", 2005.

[194] Kais Mekki, Eddy Bajic, Frederic Chaxel, and Fernand Meyer. A comparative study of lpwan technologies for large-scale iot deployment. *ICT Express*, 2019.

[195] CC1120 High-Performance RF Transceiver for Narrowband Systems. `http://www.ti.com/lit/ds/symlink/cc1120.pdf`.

[196] Chuhan Gao, Mehrdad Hessar, Krishna Chintalapudi, and Bodhi Priyantha. Blind distributed mu-mimo for iot networking over vhf narrowband spectrum. In *International Conference on Mobile Computing and Networking*. ACM, 2019.

[197] Cory Beard and William Stallings. *Wireless Communication Networks and Systems*. Pearson Education, 2015.

[198] Pei Huang, Li Xiao, Soroor Soltani, Matt W Mutka, and Ning Xi. The evolution of mac protocols in wireless sensor networks: A survey. *IEEE communications surveys & tutorials*, 15(1):101–120, 2013.

[199] James F. Kurose and Keith W. Ross. *Computer Networking: A Top-Down Approach (6th Edition)*. Pearson, 6th edition, 2012.

[200] LoRa Airtime Calculator. `https://www.loratools.nl/#/airtime`,.

[201] 32 kHz crystal oscillator.

[202] Ultra-Small Low Power, Low-Jitter, 1 Hz to 2.5 MHz Oscillator. `https://www.sitime.com/products/1-hz-2-mhz-oscillatorstcxo/sit1579`.

[203] Bernhard Korte, Jens Vygen, B Korte, and J Vygen. *Combinatorial optimization*, volume 2. Springer, 2012.

[204] Adafruit Feather 32u4 Radio . `https://www.adafruit.com/product/3076`.

[205] LoRa. `https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1272`.

[206] Y. Chen, N. Chiotellis, L. Chuo, C. Pfeiffer, Y. Shi, R. G. Dreslinski, A. Grbic, T. Mudge, D. D. Wentzloff, D. Blaauw, and H. S. Kim. Energy-autonomous wireless communication for millimeter-scale internet-of-things sensor nodes. *IEEE Journal on Selected Areas in Communications*, 34(12):3962–3977, Dec 2016.

[207] FCC Regulations. `https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet63/oet63rev.pdf`.

[208] Floris; Moerman Ingrid; Hoebeke Jeroen Haxhibeqiri, Jetmir; Van den Abeele. Lora scalability: A simulation model based on interference measurements. *Sensors*, 16(6).

[209] IoT Extends to Space. https://datacenterfrontier.com/the-iot-extends-to-space-satellite-startups-connect-remote-devices/.

[210] Latest Technology In Space Race: Satellite IoT. https://iot.electronicsforu.com/content/tech-trends/latest-technology-space-race-satellite-iot/.

[211] IoT From Space? Tracking Endangered Rhinos Via Tiny Satellites . https://www.forbes.com/sites/johnkoetsier/2020/11/17/iot-from-space-tracking-endangered-rhinos-via-tiny-satellites/?sh=3b759164684d.

[212] Internet of Things Everywhere on Earth: a satellite based M2M solution . https://cordis.europa.eu/project/id/738483.

[213] Alen Space. https://alen.space/research-and-development/.

[214] Astrocast. https://www.astrocast.com/technology/.

[215] . https://myriota.com/.

[216] AO-73. https://www.amsat.org/two-way-satellites/ao-73-funcube-1/.

[217] Toygun Basaklar, Yigit Tuncel, Sizhe An, and Umit Ogras. Wearable devices and low-power design for smart health applications: Challenges and opportunities. In *2021 IEEE/ACM International Symposium on Low Power Electronics and Design* (*ISLPED*), pages 1–1, 2021.

[218] Feng-Ru Fan, Zhong-Qun Tian, and Zhong Lin Wang. Flexible triboelectric generator. *Nano Energy*, 1(2):328–334, 2012.