A Comparison of the Energy Consumption Properties of Wi-Fi Backscatter and Bluetooth Devices as it Relates to Sensor and Asset Tracking Solutions

A Technical Paper prepared for SCTE by

Ty Pearman
Principal Engineer
Comcast Labs, Comcast Cable
4100 East Dry Creek Rd
Centennial CO 80122
ty_pearman@cable.comcast.com

Arun Ravisankar
Principal Engineer
Comcast Labs, Comcast Cable
1800 Arch St, Philadelphia PA 19103
215-286-7558
Arun_Ravisankar@comcast.com

Table of Contents

List of Figures

List of Tables

UNLEASH THE
POWER OF LIMITLESS
CONNECTIVITY
VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall
Technical Forum
SCTE • NCTA • CABLELABS

1. Introduction

The airwaves around us are continually filled with the invisible signals emanating from and between the Wi-Fi gateways and devices that use them for broadband connectivity, as well as from and between devices that use Bluetooth for connectivity. Naturally, techniques like Radio Frequency Identification (RF ID), which date back to the 1970s, were developed to use those radio waves for object identification. Commonly, you will see RF ID tags affixed as stickers or built into consumer devices, for the purposes of being read at a distance and without line of sight, as with highway toll readers, employee ID badges, etc. The ambient nature of these signals provides the opportunity to "piggy back" on the existing networks, which can reduce the overall power consumption of RF backscatter solutions. This paper examines the performance tradeoffs between different communication protocols used in both sensor and tracking solutions, including RF backscatter, Wi-Fi, Bluetooth, and LoRa (Long Range). The main area of focus will be around power consumption and data throughput for IoT type solutions. Readers will learn the basics of energy consumption and data transmission rate capabilities from these technologies, along with the power consumption baselines of mainstream IoT devices and how transmission protocols can impact the powering and life of the IoT devices.

Cable network operators are always looking for ways to add services for their customers, especially so since the 1990s. A couple of examples include: Data over cable, voice, and DVR(Digital Video Recorder) evolving to nDVR, were added to the service bundle. More recently, home monitoring and security services have also been offered by many operators. [1]
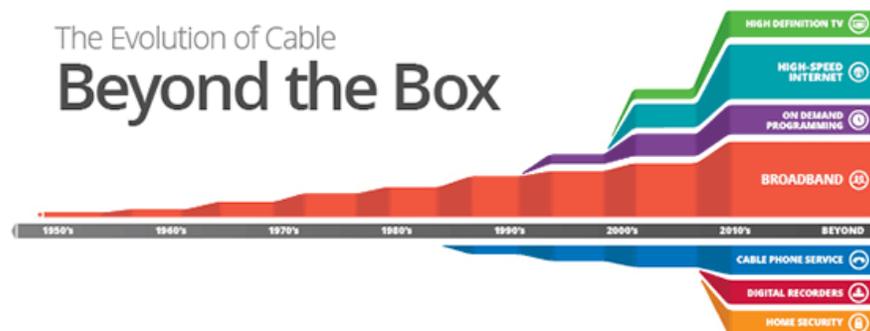
(Calcable.org, n.d.)

Figure 1 - Evolution of Cable

The Internet of Things is loosely defined as Internet-connected sensors in homes, businesses, and public spaces, as well as the data analytics monitoring of those sensors back in the data center. With the Internet of Things, there is an opportunity to rapidly open up entirely new service opportunities that can differentiate cable network operators from their competition. However, the primary challenge will be to smoothly install, operate and integrate these new services with the operator's existing service bundle.
Cable network operators are uniquely positioned to offer IoT services to new and existing customers. They have four characteristics that industry start-ups and OTT service providers covet:
- Existing service location in millions of homes, businesses, and public spaces

- High speed and reliable network connectivity
- Power for sensors and gateways
- An existing and localized/in-market fleet of fulfillment technicians

Cable network operators have a well-established presence in the home including cable modems, home gateways, set top boxes, Wi-Fi extenders and home security hubs, however the evolution to new services - such as connected healthcare, and smart homes – will require new devices and sensors, as well as increased care to ensure the highest network performance while preventing security breaches.

Where is the world of IoT going? According to a market report from Research and Markets "The total number of IoT connection worldwide will increase from 1.5 billion at the end of 2019 to 5.8 billion in 2029". Using that as a data point one can assume these devices will continue to show up in our daily lives in various locations, in a multitude of forms. Many of these devices are part of larger systems or add-ons to existing systems. In those cases, the powering of the devices come from wired sources or systems recharged on a regular basis. Additional implementations consist of stand-alone devices used for monitoring or tracking. These devices tend to be small and powered by batteries (think of door sensors, window sensors, outdoor sensors for temperature, humidity, noise…etc.). One of the biggest issues with the stand-alone IoT devices is maintaining power to the devices so they can do their job.

For systems or environments with large amounts of sensors, replacing batteries can be an endless task, making the labor cost to replace batteries or devices a non-starter. Just think about how often you swap out your remote batteries and multiply that by 5, 10 or even more for your home IoT devices. Now take that equation and move it to an outdoor or warehouse situation and the problem explodes one or two orders of magnitude. With that said, many IoT vendors target their designs to a single battery that will last the lifetime of the device, which can be anywhere from 3 years all the way out to 10-15 years in a low power wide area network solution (LPWAN).

So how can we extend the life of these devices? Doing so could be a game changer, depending on the application and the amount of data that is being sent out. There are a couple of ways this can be done: use larger batteries, leverage energy harvesting technologies to replace the batteries or extend battery life tend to be the most obvious. However, another interesting option is changing the data transmission protocol used to transmit the data to the access point/base station.

2. Communication Protocols used in IoT(Internet of Things)

IoT devices are ubiquitous and are part of our everyday life, from the smart home devices we use to the health and wellness devices that keep track of our overall health. Have you ever wondered what makes these devices smart? The simple answer is that these devices are now capable of communicating with a computer/machine/internet and provide critical data for algorithms and applications.
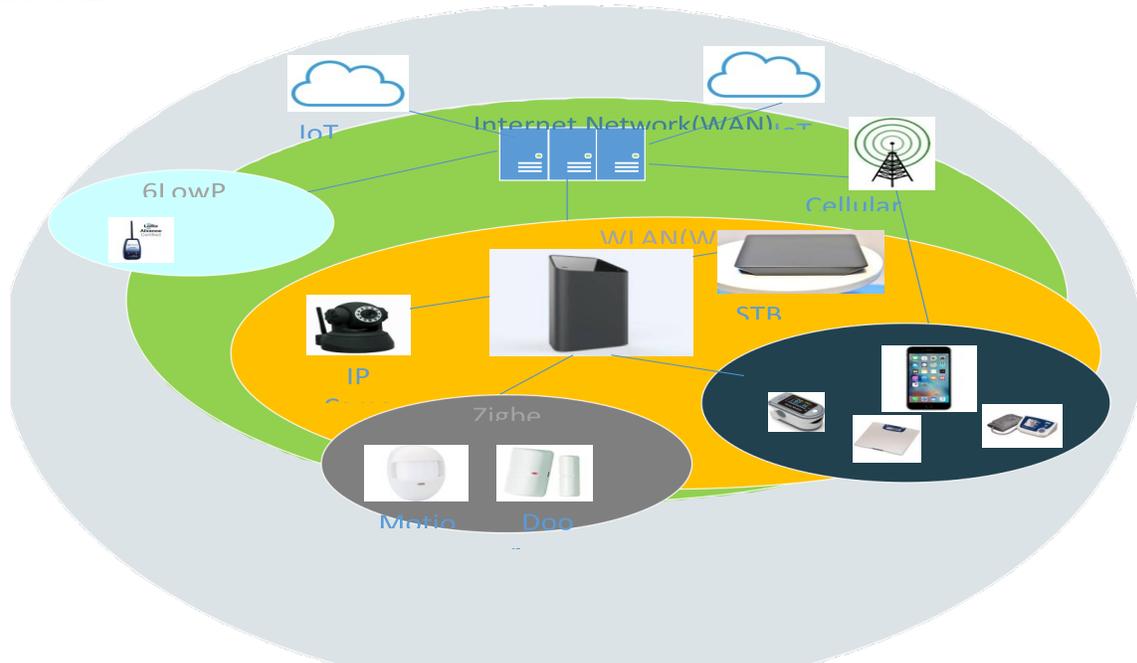
Figure 2 - Devices and Networks used on IoT Applications

Figure 2 shows multiple devices using different communication networks and protocols. The choice of the protocols and networks depends on the type of data involved, range of the sensors, and the applications these devices support. Some networks and protocols support data transfer at longer distances, while other protocols support larger data transfer rates at low range(distance). Depending on the range, these networks could be classified as WAN(Wide Area Network) or PAN(Personal Area Network). PAN includes networks like Bluetooth, Zigbee, Wi-Fi, which support very high data transfer rates, but their range is limited to probably a few meters. On the other hand, WAN include networks and protocols like LoRaWAN, NB-IoT, Mobile(LTE/5G), Cable/Fiber broadband, and can support connectivity at larger distances. Table 1 provides some key details of each of these network protocols. The sensor that uses these networks need to meet the power requirements of the network/protocol, as the sensor might need to engage the antenna and provide enough power to transmit and receive the data. Often, the power characteristics would depend on the data being handled and the distance the data is being transmitted.

IoT Protocols	• Zigbee • Thread • BLE • Matter
Wide Area Network	• LoraWAN • Mobile(LTE,5G) • Cable/Fiber Broadband
Personal Area Network	• WiFi • Bluetooth/BLE • Zigbee • ZWave • NFC
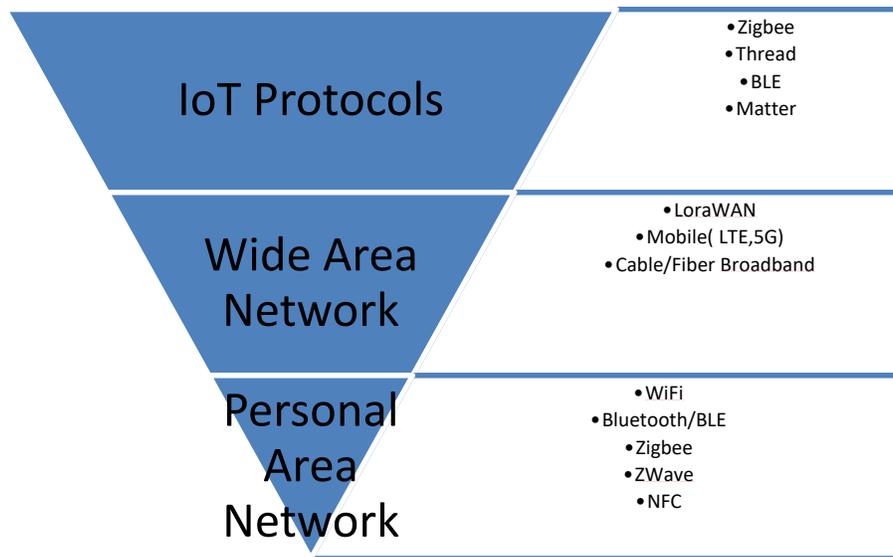
Figure 3 - Components of a typical IoT Application, Networks and Protocols used

As the penetration of these sensors/devices increase, it is critical to note the power consumed by these sensors, both from an efficiency and a sustainability perspective. Most of these sensors are often powered by batteries and the users would ultimately need to replace batteries on these sensors. This is a significant challenge in terms of a sustainable ecosystem. This paper compares the power characteristics of the different protocols and would seek methods to make the IoT ecosystem more sustainable. By understanding the power characteristics and requirements for these networks and protocols, we can explore augmenting the power from sustainable sources, such as ambient light. This would improve the battery life of the sensor, making it more sustainable and provide better customer experience.

Table 1 - Table showing operating conditions of IoT networks

	Personal Area Networks						Wide Area Networks	
	NFC	**BLE**	**Wi-Fi**	**Zigbee**	**Zwave**	**WiFi HaLow**	**Mobile(LTE, 5G)**	**LoRa**
Operating Freq	13.56 MHz	2.4 GHz	2.4, 5 and 6 GHz	2.4 GHz	908.42 MHz	< 1GHz	450 MHz to 6GHz and 24.25GHz to 52.6 GHz	902-928 MHz
Max Power	Low power needed	1mW – 100 mW	100mW – 4000mW	10mW – 100mW	10mW – 100mW	10mW – 100mW	Varies as per endpoint	
Battery Operated?	Yes	Yes	Possible	Yes	Yes	Yes	Yes	Yes
Range	10 cm	<100m	Around 50m	<100m	100m	Approx 1Km	Range varies. Up to a few Km. 5G bands offer very low range compared to LTE	Between 15 to 20 Km
Throughput	424 Kbps	2Mbps	WiFi ax max – 3.5Gbps	250kbps	40kbps to 100kbps	150kbps to 4Mbps	50Mbps to 10Gbps	300 bps to 37.5 kbp
Ease of Adaptation	Wide Adoption	Wide Adoption	Wide Adoption	Wide Adoption	Medium Adoption	Low Adoption	Growing Adoption	Low to Medium Adoption

3. Power Characterisctics

Table 1 provides us with some details on the metrics on the networks and protocols used. In this section, we will examine how some of these protocols are efficient with regard to power consumption.

As the world around us gets more complicated, the flow of information grows in importance as we become more connected. Someone is always checking their Facebook feed, e-mail, doggie cam, receiving alerts from their home systems, finding their car, checking the air quality, traffic speeds…etc. As the flow of information becomes increasingly more important for our daily lives, the need for these systems to be connected and always available becomes critical. The devices that make it all possible need to rely on some type of power source to keep us "in the know".

The easiest power solution for all these are the devices already connected into the regular power grid. With wired solutions, the power usage isn't a big concern, other than a power outage, which can be handled by some type of battery backup, if necessary. Other solutions that tend to be more mobile (the main one being a smartphone) have rechargeable batteries that give the device portability but offer a very limited life before the user must recharge the system. The final case, which we are most interested in, is the IoT case where devices are deployed in a stand-alone fashion and expected to function for an extended period normally measured in years as opposed to days. This is where changes in power consumption can have enormous impacts on the life of the device.

There's a couple of ways to break down the power characteristics of the different devices and protocols. In general, the farther you transmit a signal, the more power you will need; the more data you transfer, the more power you will need; and the longer the device is "awake" and transmitting data, the more power you will need. This addresses the technologies employed with a very broad stroke, but with that in mind, we can break the different solutions down based on their reach, reliability, throughput, and power consumption. Each of these different parameters really speaks to the notion of there not being a "one size fits all" IoT solution.

In general, IoT devices have two main purposes: the first is to collect data and the second is to forward that data to a centralized system where the data can be stored, analyzed, and/or acted upon. Looking at the power budget for the endpoint, a large portion is expended in the transmission of the data back to the gateway. These networks consist of many endpoints to very few gateways. In some cases, a gateway can support up to and potentially over 1 million IoT devices. Here's some of the different networks these IoT devices can be deployed in:

3.1. Personal Area Networks(PAN)

PAN is a network that interconnects computers within a limited area such a residence or a small business facility. Primarily these networks were intended to be the data pipe between computers and modems and hence the focus was more on data throughput. As spaces like residences and businesses grew, the need to provide reliable data connectivity at larger distances became important. This resulted in increased power output on the radios. With the advent of IoT devices and networks, devices that are powered by batteries grew and this put a natural limit on the power we could transmit. There have been significant advancements on the power efficiency of these networks that consume less power, but still manage to support better data rates.
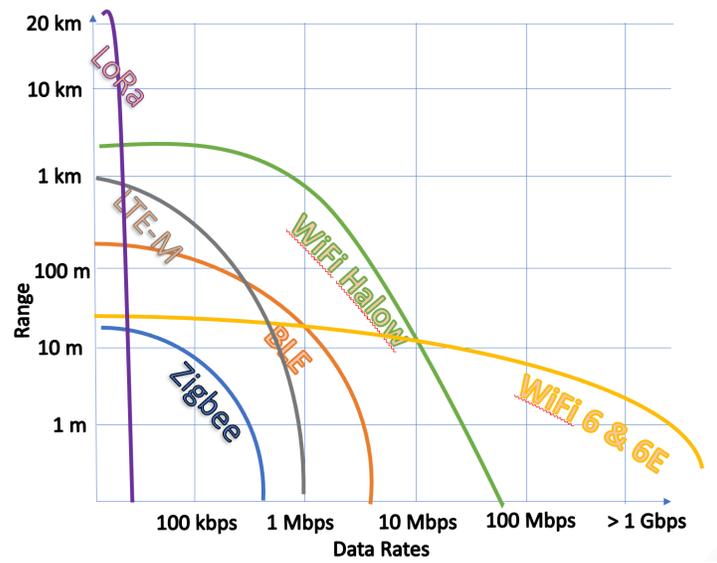
Figure 3 - Range vs Data rates of Wireless PAN

As shown in Figure 3, we see that the data throughput of the networks tends to drop down as the distance between two endpoints increase. The data rates supported at different distances depends on the protocol used and on the specific implementation of the standard. As protocols are pushed to the edge, the need to provide reliable connectivity often results in increasing the output power, which in turn puts a lot of stress on the endpoints, especially if they are battery-powered. Even within range, the pain point in managing battery life of multiple sensors and devices leads to an unpleasant customer experience. Hence, this paper looks at the power characteristics of these network protocols and where power performance can be optimized if we can augment the battery power with energy harvested from ambient power sources, like light, temperature differential, and power over RF. We will look at the power characteristics of some protocols in this section.

- **BLE (Bluetooth Low Energy)**
  Compared to Classic Bluetooth, Bluetooth Low Energy is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range. Mobile operating systems including iOS, Android, Windows-Phone and BlackBerry, as well as macOS, Linux, Windows 8, and Windows 10, natively support Bluetooth Low Energy.

  A typical BLE SoC (i.e. an all-in-one Application + Radio chip) typically consumes:

    - A few hundreds nA(Nano Amp) while in deep sleep,

    - 2 to 10 µA while a RTC tracks time (needed between radio events while advertising or connected),
    - 10 to 30 mA while CPU or Radio runs (computing data, TX, RX). RX and TX power consumption is roughly the same.

  The life of a BLE peripheral basically consists of 3 main states:

- Be idle (not advertising, not connected). The device would be in a sleep/standby state and consumes just over a few hundred nanoamps though.

- Advertise (before a connection takes place). Peripheral needs to be running approximatively 5ms every 50ms. This is the time when your device actually uses the most power because advertising requires sending many packets, frequently. Average power consumption is in the 1-10 mA range.

- Be connected. Here, consumption is application-dependent. If application is mostly idle, a peripheral is required to wake up periodically and must send a packet each time in order to keep the connection alive. Even if the peripheral has nothing useful to send, an *empty packet* is still sent. Side effect: that means low duty cycle applications basically transmit packets for free.

We could estimate the battery life of a BLE device using a typical BLE example:

- Radio power consumption = (5.4uA * 3V) * 1/2s = 8.1uW

- System power consumption = (2uA * 3V) = 6uW

- Total power consumption = 14.1uW

- Battery life = ((300mAh * 3V) / 14.1uW) * 0.7 = 44681 hours = 1860 days

If we can augment the battery with an energy harvesting source that can supply enough power for the SOC, we could either make the sensor battery free or extend the battery life.

- ***ZigBee***
  ZigBee is a mesh network protocol designed to carry small amounts of data across medium distances. It runs on a mesh topology network, meaning information from a single sensor node, travels across a group (or "mesh") of nodes until the transmission reaches the gateway.

  ZigBee is a local area network (LAN), so unlike BLE, it is not intended to connect to devices directly around a user. Instead, it connects to devices that need a wider range. Because of this, it's an ideal protocol for home automation[1] and smart lighting[2].

  As an example, battery life of a motion sensor with a ZigBee radio could be around 5-7 years, which is comparable to that of BLE

---

[1] https://www.link-labs.com/applications-of-home-automation/
[2] https://www.link-labs.com/smart-lighting/

- **WiFi HaLow**

  WiFi HaLow is IEEE 802.11ah standard that uses the WiFi protocol characteristics, using a sub-GHz band. WiFi HaLow promises
    - Lower Power Consumption
    - Longer Distances
    - Better Penetration
    - Lower data rates (150 Kbps at longer range, 10+Mbps at closer range)

  Figure 4 shows the frequency bands used by WiFi Halow in the WiFi standards.
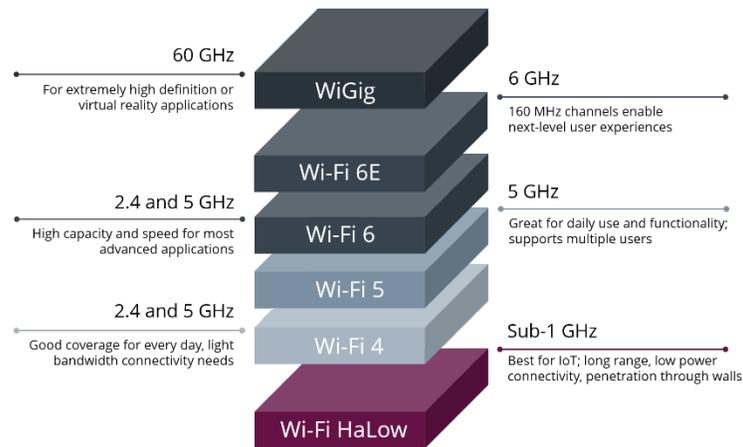
Figure 4 - Wi-Fi Frequency Bands

3.2. Wide Area Network (WAN)

(In the context of this paper, when talking about WAN, we are referencing wireless WAN solutions.)

Some of the most compelling deployment use cases for IoT revolve around the deployment of sensors and asset tags spanning large geographic reach (when the term WAN is used, a range of more than 2km is a good starting point). There are a multitude of use cases for these devices, but in general they can be categorized into a handful different areas…1) highly reliable data with large data throughput requirements, 2) small amounts of data that are not time sensitive and 3) small amounts of data requiring a high level of reliability. Additionally, from a technology perspective, there are two different solutions that are usually discussed for these transmission scenarios; cellular and non-cellular (sometimes referred to as licensed and unlicensed spectrum). Below is a chart that outlines some of the different characteristics of these systems

Table 2 - Characteristics of Cellular and Non-Cellular LPWAN Networks

Parameter	CAT-1	CAT-M1	NB-IoT	LoRa	SigFox
Bandwidth	1.4 - 20 MHz	1.4 MHz	180 kHz	125 kHz or 500 kHz	100 Hz
Data Rate	DL: 10 Mbps UL:5 Mbps	DL: 1 Mbps UL: 1 Mbps	DL: ~20 kbps UL: ~60 kbps	.3 – 50 kbps	100 bps
Latency	50-100 ms	10-15 ms	1.6 – 10 s	Topology dependent	Topology dependent
Spectrum	Licensed	Licensed	Licensed	Unlicensed	Unlicensed
Peak Transmit Power	23 dBm	23 dBm	23 dBm	20 dBm	22 dBm

- Cellular (Licensed spectrum)[3]
Cellular WAN solutions have evolved with the changing cellular technologies, but the most common ones are CAT-1, CAT-M1 and NB-IoT. All three solutions leverage licensed cellular bands which provide a more controlled environment for the transmissions which give the data transmissions a higher reliability than networks using unlicensed spectrum.

    - CAT-1
    In the world of LPWAN CAT-1 would be considered a power hog but has some of the highest throughputs and lower latency.

        ◊ Latency typically 50-100 ms
        ◊ Throughput of 5 Mbps uploads and 10 Mbps downloads
        ◊ Spectrum bandwidth of up to 20 MHz

---

[3] https://en.wikipedia.org/wiki/Narrowband_IoT

◊ Typical use cases include video surveillance, ATM communication and vehicle telemetry

- CAT-M1(LTE-M)

CAT-M1 or LTE-M uses existing LTE networks but consumes far less battery power than CAT-1 devices. The solution has the ability to handle moderate bandwidth applications with minimal latency requirements.

◊ Latency typically 10-15 ms
◊ Throughput of 500 kbps uploads and 1 Mbps downloads
◊ Spectrum bandwidth of up to 1.4 MHz
◊ Ability to handle cell tower handoffs
◊ Typical use cases include wearables, high value asset tracking and health monitors

- NB-IoT[4]

This protocol is designed for devices that transmit small amounts of data with fairly loose latency requirements. The solution still leverages the LTE network, but operates in the roll off of the licensed spectrum.

◊ Latency typically 1.6 – 10 seconds
◊ Throughput of 120 kbps uploads and 160 kbps downloads
◊ Spectrum bandwidth of approximately 180 kHz
◊ Typical use cases include smart gas, water and electric meters along with smart city applications such as street lighting and parking sensors
◊ Stationary application since it cannot handle cell handoffs

Table 3 - LPWAN Network Characteristics

	Data reliability	Data throughput	Power consumption	Endpoint mobility
Grid Powered Cellular	High	High	High	stationary
Battery Powered Cellular	High	Low	Medium	
LPWAN/NB-IoT	Low	Low	Low	broad

- Non-Cellular (Unlicensed spectrum)
  In the unlicensed LPWAN space the main technologies used are LoRa and Sigfox. Both solutions are focused on data uplink, where a large number of sensors transmit data to a small number of gateways in a star type topology. With these solutions using unlicensed spectrum, interference in the form of noise and other signals is a much larger concern.

---

[4] https://www.siretta.com/2021/02/lte-cat-1-vs-lte-cat-4/

Data collected and used in these systems in most cases is slow changing and not latency dependent. Occasional missed data packets shouldn't impact the overall system. Applications like temperature monitoring, air quality and agricultural data are good candidates for both solutions.

- LoRaWAN or LoRa[5]

LoRa networks can be deployed in a very low-cost manner with a minimal number of gateways to support the network. Unlike licensed LPWAN solutions, network gateways are easily deployed and managed. With a focus on low power LoRa endpoints can see device lifetimes from 10-15 years depending on the data being transmitting, frequency of data updates and distance the sensor is from the gateway.

  ◊ Latency of system is dependent on the number of packets a gateway can process in a day related to the number of endpoints being supported
  ◊ Throughput of .3 kbps to 50 kbps
  ◊ Easily transmits through physical barriers
  ◊ Spectrum bandwidth of 125 kHz or 500 kHz uplink and 500 kHz downlink
  ◊ Star on Star network topology

- SigFox[6]

SigFox uses a proprietary technology which is optimized for extended distance over LoRaWAN, where up to 10 km is urban and 40km is rural areas, where LoRaWAN would only be capable of roughly 5 km in urban and 20 km in rural areas.

  ◊ Latency of system is dependent on the number of packets a gateway can process in a day related to the number of endpoints being supported
  ◊ Throughput max of 100 bps
  ◊ Easily transmits through physical barriers
  ◊ Spectrum bandwidth of 100 Hz for the uplink and 600 Hz on the downlink
  ◊ Star network topology
    ◊ Limited to 140 messages a day for the uplink and 4 messages for the downlink

---

[5] https://lora-alliance.org/about-lorawan/

[6] https://www.survivingwithandroid.com/sigfox-protocol-network-architecture-iot-protocol-stack/

4. Energy Harvesting

Harvesting energy for IoT applications can done using a variety of sources. While some include using the ambient environmental conditions to harvest energy, other methods include transmitting energy using mediums like WiFi or RF. Candidates include sensors used in IoT applications such as temperature, humidity sensors, to motion sensors and cameras. The key here is to find the right energy source that can either power the sensor in a battery-free mode, or trickle-charge the batteries to increase the overall life of the sensor.

Figure 5 shows an example of a system that is capable of harvesting energy to augment the battery of a sensor using the BLE communication system.
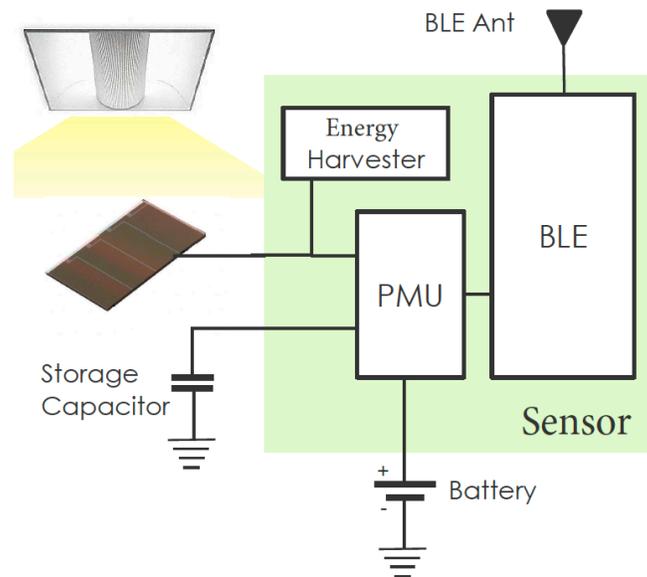
Figure 5 - Typical Energy Harvesting system

There are a variety of energy sources from which we could harvest energy. We will examine a few of the most application or common energy harvesting technologies next. Figure 6 illustrates how different energy harvesting technologies could support applications such as sensors, asset tracking application and many others. Table 4 shows the power density of the each of the energy harvesting technologies.

RF 🛜

TV Remote

PV 💡

Asset Tracking

Keyboard

ESL   Beacon

Sensing   Wearable

Switch/Control

Mechanical 👆   Thermal
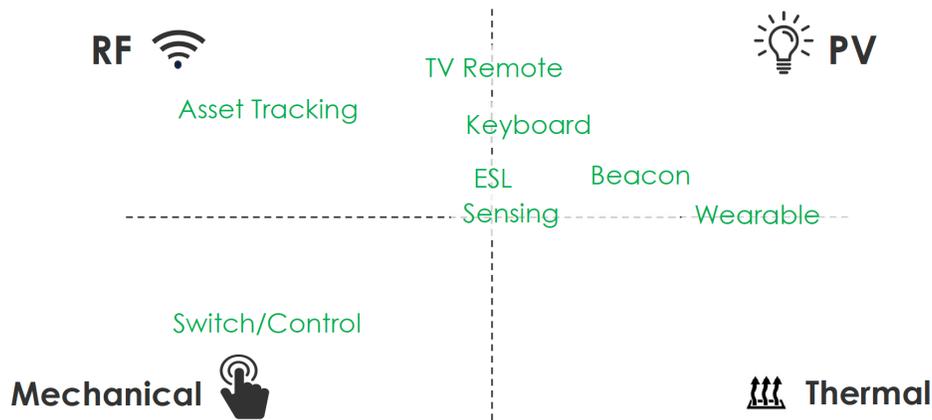
Figure 6 - Applications Supported by Energy Harvesting Technologies

Table 4 - Power density of various Energy harvesting systems

Source	Power Density
Mechanical/Piezoelectric	[0.11-7.31] mW g_2/cm$_3$
Radiofrequency	$1.2*10^5$–15 mW/cm$_2$
Solar	[0.006–15] mW/cm$_2$
Thermoelectrical	[15–60] W/cm$_3$
Wind	[0.065–28.5] mW/cm$_2$

4.1. Photo Voltaic Energy Harvesting

The technology of using photons (sunlight) for generating power/energy has been around for millions of years. The ambient light available around us, even indoors, is sufficient to generate energy that can trickle charge a battery or power low-power sensors. Significant progress has been made in the form of organic photo voltaic cells that can generate sufficient power from indoor lighting conditions.

Figure 7 shows the power needed for various wireless protocols and how they could be powered by a 10 cm^2 IPV (Indoor Photo Voltaic) panel.

UNLEASH THE
POWER OF LIMITLESS
CONNECTIVITY
VIRTUAL EXPERIENCE
OCTOBER 11–14

2021 Fall
Technical Forum
SCTE • NCTA • CABLELABS
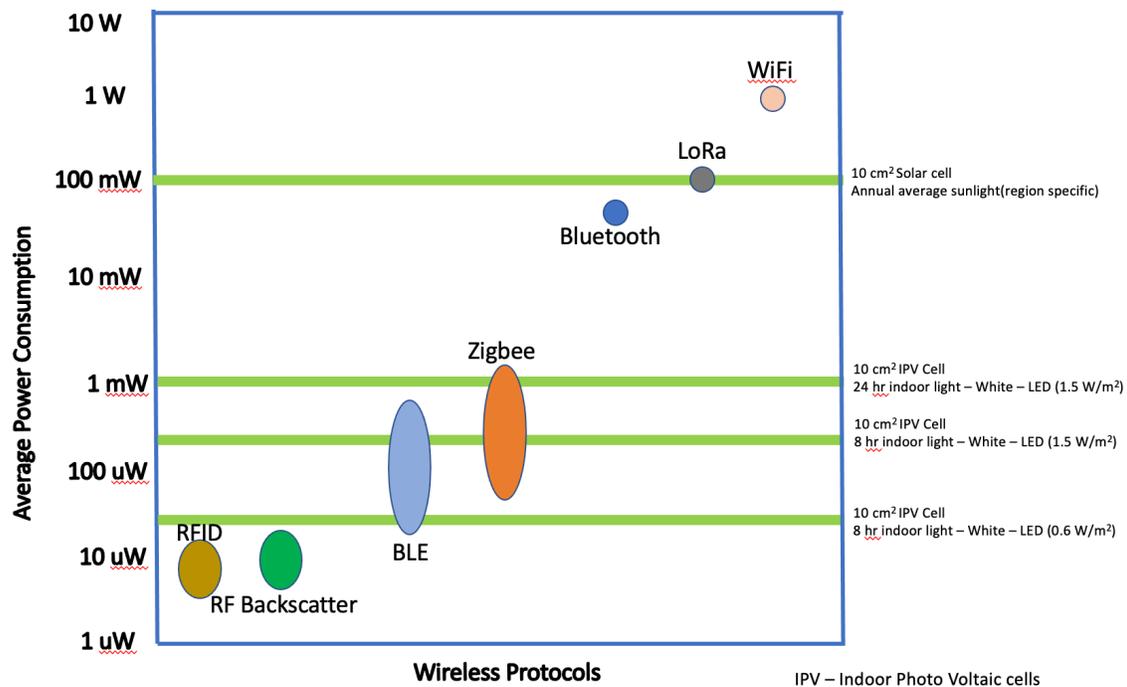
Figure 7 - Mapping wireless protocols to indoor photovoltaic cells based on power needs

4.2. Radio Frequency based Energy Harvesting

RF-based energy harvesting provides a controlled environment for charging/powering IoT devices/sensors over RF/Electromagnetic waves that propagate around us in the form of WiFi/Bluetooth or other wireless signals. RF-based energy harvested signals can carry the information along with the production of energy and can also process that information simultaneously. [7][8]The amount of RF energy available for harvesting at the RF harvester's antenna input will depend on the source's transmitter strength, RF frequency, duty cycle, and range to the receiver.

Figure 8 shows a typical RF harvester that receives energy on a particular frequency. There can be 2 types of RF harvester.

- Ambient RF harvesting: In this case, the receiver is capable of harvesting energy from ambient RF like Bluetooth and WiFi signals
- Active RF harvesting: In this case, a transmitter would send energy on a specific frequency and the receiver would tune to get power. This method offers a more controlled environment.

---

[7] https://ieeexplore.ieee.org/document/6552840 - **Relaying Protocols for Wireless Energy Harvesting and Information Processing**

[8] https://ieeexplore.ieee.org/document/6623062 - **Wireless Information and Power Transfer**
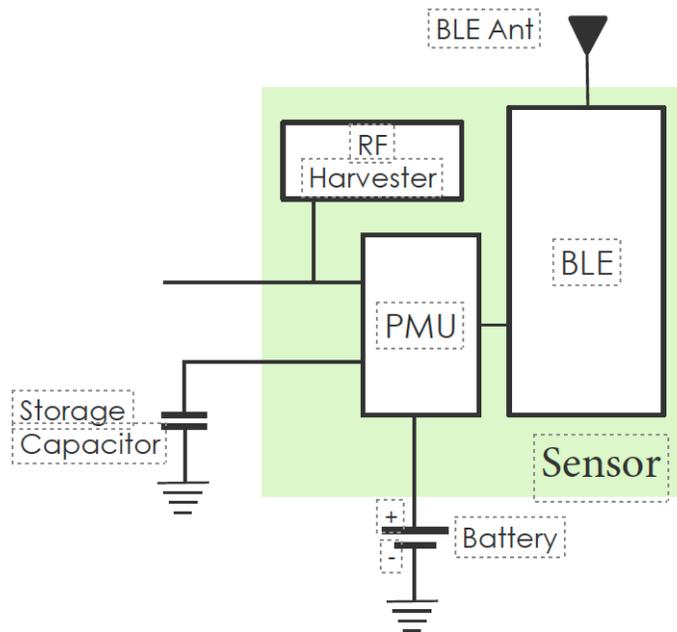
Figure 8 - RF based Energy Harvesting
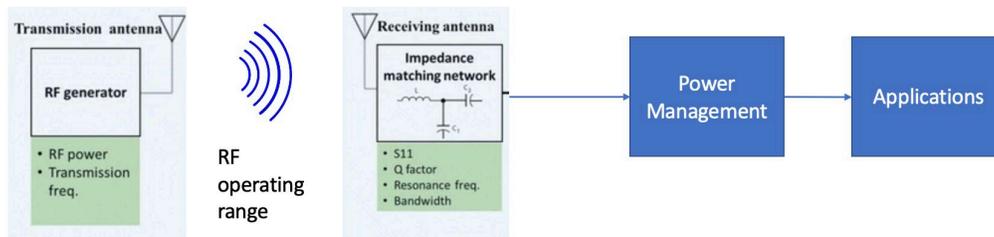
Figure 9 - Active RF based Energy Harvesting

4.3. Mechanical based energy harvesters

Devices called Nanogenerators can convert small amounts of mechanical energy into electric current. The very first nanogenerators were based on the triboelectrification and piezoelectric effect.[9]

Energy harvested from unintended mechanical vibration and abandoned heat can also be directed to low powered electronic devices. Conversion of energy from the ambient environment into electrical energy is known as vibration energy harvesting (VEH).[10]

---

[9] https://science.sciencemag.org/content/312/5771/242

[10] https://www.ingentaconnect.com/content/tandf/ginf/2019/00000201/00000001/art00010;jsessionid=35omsvrame402.x-ic-live-01

4.4. Thermal Energy Harvesters

Thermal energy harvester use "heat" and temperature variation as the main source to generate power. Two techniques are being used to harvest energy from a thermal source. The first is pyroelectric and the other is thermoelectric.

- The Seebeck effect[11] is used by the thermoelectric technique to convert the difference in temperature into usable energy forms directly. A 5–8% efficiency of harvesting is achievable by the thermoelectric technique of harvesting.
- In pyroelectric energy harvesting, the wasted heat energy is converted into electrical energy for battery-free IoT-based portable devices and wireless sensors. It can convert temperature fluctuations into electrical energy, and this makes it more attractive for harvesting energy.

5. Case Study

As discussed in the earlier section of this document, it is very important and critical that we innovate technologies that help us maintain the growing number of IoT devices and also provide a sustainable solution. Increasing battery usage creates challenges in recycling them. In the sections above we looked at how networking technologies, both PAN and WAN perform. As the number of endpoints and sensors grow, reliable communication at farther distances is a challenge. Increasing output power not only increases draw on the energy sources, but increases the noise in the system and makes it more susceptible to noise.

In this section, we look at technologies that can offer a low-power alternatives to some of the wireless PAN technologies. We will look at the network performance in terms of data throughput, range, efficiency, latency, and power consumption. As a case study, we look at RF backscatter technology to see if it has potential as a low-power, protocol-agnostic, secure network that could be used by IoT sensors to transmit data and stay connected.

5.1. RF Backscatter Network

In RF backscatter networks, multiple network topologies are possible. We will look at a few of those topologies, and one in detail, to evaluate its effectiveness in terms of data throughput, efficiency, and latency.

- Ambient - In the first network topology, the endpoints (backscatter devices) communicate with each other by reflecting either ambient signals or a dedicated carrier service, as shown in Figure 10. The challenge with this network topology is that the receivers exhibit poor sensitivity in the range of -40 to -60 dBm, which limits the operating distances between the endpoints.

---

[11] https://en.wikipedia.org/wiki/Thermoelectric_effect

UNLEASH THE
POWER OF LIMITLESS
CONNECTIVITY
VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall
Technical Forum
SCTE • NCTA • CABLELABS
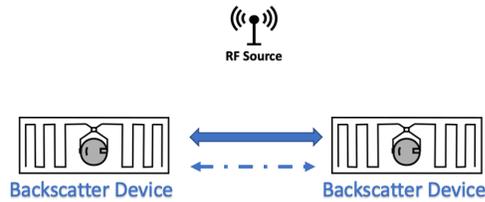
Figure 10 - Backscatter network using Ambient signals

- WiFi/LoRa: The second backscatter topology involves receiving backscattered packets on commodity radio receivers like WiFi or LoRa as shown in Figure 11. This topology is a significant improvement from the ambient backscatter, as the WiFi/Bluetooth/LoRa radios have better sensitivities. Using a LoRa receiver can further extend the range to 100s of meters.
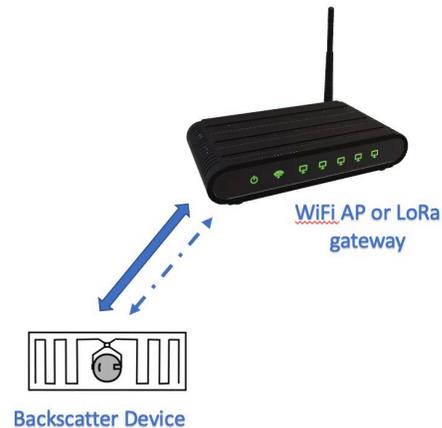
Figure 11 - Backscatter using Wi-Fi or LoRa signals

- Full Duplex: The third topology uses custom signal sources and custom receivers in a full-duplex configuration to operate the backscatter devices as shown in Figure 12. This configuration provides maximum flexibility.
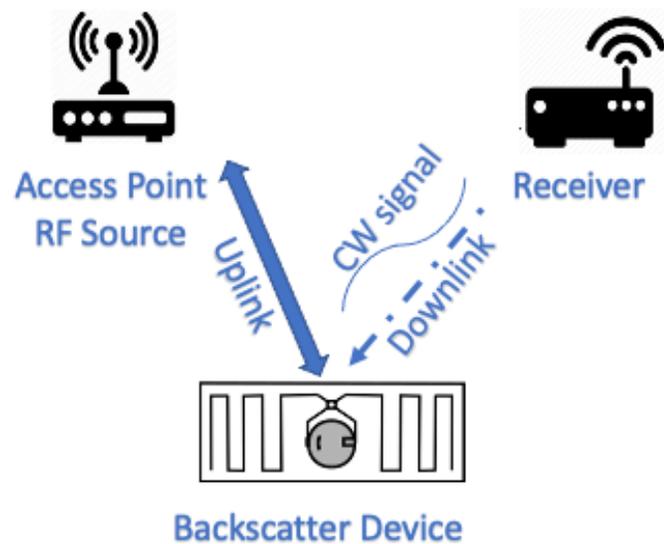
Figure 12 - Backscatter using Custom RF sources

While backscatter can be used with batteries, RF harvesting is still a popular choice for building battery-free systems since we can use the same antenna for both power and communication. Backscatter research is still in its infancy with primary focus on novel physical layer design. Recent research proposes solving some of the pressing networking and MAC-layer challenges of backscatter.[12]

Unlike a traditional wireless network that consists of solely a transmitter and a receiver, a RF Backscatter network consists of three distinct device roles: an Endpoint, a Gateway, and a Companion.

- **_Endpoint_**
  The Endpoint a tiny, low cost, low power device that would be a sensor (such as a temperature sensor or smoke detector). The endpoint in a typical network (using WiFi/BLE) would have a wireless transmitter. However, in a backscatter network topology, the sensor achieves low power connectivity by using a backscatter uplink to transmit data packets to the gateway, as shown in Figure 12.

- **_Gateway/Access Point_**
  The Gateway in this backscatter network takes the role of a traditional wireless receiver. It acts as a data sink for backscatter packets that are sent in from multiple endpoints. The gateway also serves as a bridge/hub between the backscatter network and another PAN or WAN or cloud server that can process the data generated by the endpoints. The gateway is shown as the RF source in Figure 12.

---

[12] M. Hessar, A. Najafi, and S. Gollakota. Netscatter: Enabling large-scale backscatter networks. In NSDI 19

- *Companion/Receiver*
  The companion enables Backscatter communication by transmitting a brief CW (Continuous Wave) signal for each uplink transmission. The companion also coordinates Endpoint devices using a low power downlink signal.

In this network topology, the communication is initiated by the Companion. The companion first transmits a wake code to an Endpoint using On-Off Keying (OOK)[13] modulation. The Endpoint has an ultra-low power detector that helps it detect the wake code. Upon receiving the wake code, the Endpoint goes into a listening state/mode. An Endpoint in listening state would be able to receive data from the Companion via the downlink.

The Companion then transmits a downlink packet followed by a brief CW signal. The downlink packets instruct the Endpoint to transmit a backscatter packet during the subsequent CW signal. By selectively reflecting and absorbing the CW signal from the companion, the Endpoint is able to use backscatter to synthesize a wide variety of standard RF protocols (WiFi/LoRa) that can be received by the Gateway.

The Gateway can then bridge the data coming in from the backscatter network to a server that can process the data. Figure 13 shows the sequence followed by a backscatter network to transmit data from a sensor to an app on the customer's phone. Since the sensor/endpoint consumes low power, we could as well add any energy as discussed in the Energy Harvesting section of this paper.
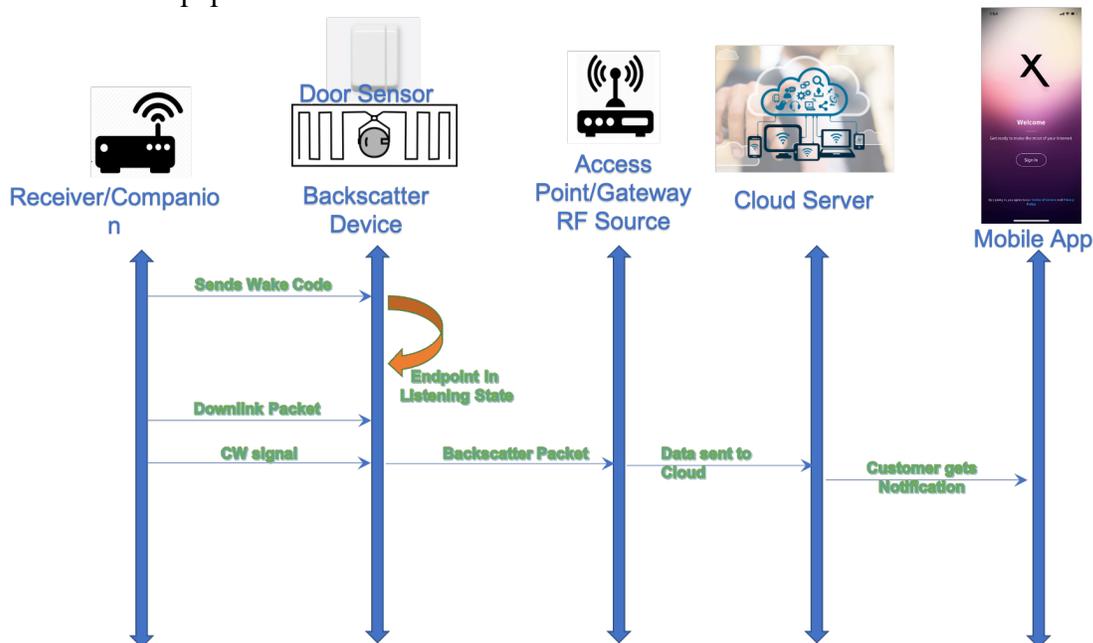
Figure 13 - Sequence diagram of a RF backscatter network packer transmission

---

[13] https://en.wikipedia.org/wiki/On%E2%80%93off_keying

RF Backscatter endpoints can achieve extremely low power to transmit the data generated by the sensor. A conventional radio actively generates and transmits RF signals for communication. Such system requires complex hardware and uses significant amounts of energy. See the comparison of power consumed, shown in Figure 7. Backscatter modulation utilizes reflected RF signals to communicate, which dramatically reduces all the systems needed to generate radio signals directly at an endpoint/sensor.

The reflections are produced by modulating the Endpoint's antenna impedance in the presence of a CW (Continuous Wave) signal, generated by the Companion. See Figure 14, when any type of wave encounters a boundary between two mediums that have different impedances, a portion of the wave is reflected. The reflection's magnitude is determined by the difference in impedance between those mediums. This is true for a mechanical wave traveling through a rope to a fixed point on a wall, or an electromagnetic wave encountering an antenna.
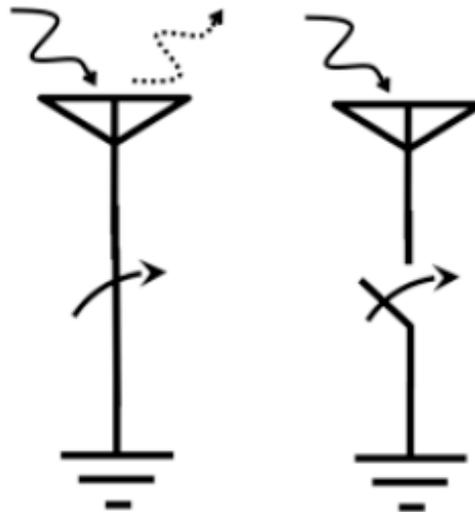
Figure 14: RF wave reflected/absorbed due to change in impedance

6. Conclusion

The world around us is becoming more connected on a daily basis; it is easier than ever today to grab information about the weather in your favorite destination, the air quality in your neighborhood, if you left a window open or a door unlocked and if you need to water your grass. In many of these cases, battery-powered IoT devices and their networks are supplying this information, but to keep the information flowing, these devices need to stay powered up and there's only so many options available. This paper has outlined some of the potential design considerations that could be implemented to extend the life of these devices either through improving the energy efficiency of the protocols used or additional technologies that could replace or extend the battery life of these IoT devices. In IoT applications and networks, where devices are deployed in a stand-alone fashion and expected to function for an extended period

normally measured in years as opposed to days. This is where changes in power consumption can have enormous impacts on the life of the device.

Innovation has been a constant in this industry, as we strive to bring in brand new technologies or improve existing ones to accommodate more use cases and help manage the ever growing number of battery-powered IoT devices.

The energy harvesting technologies mentioned in this paper have been deployed for many decades, and continue to evolve to address the pressing needs of a fast changing world.

The RF backscatter solution presented in this paper is promising and enables us to consider an ultra-low power, protocol-agnostic sensor portfolio.

Abbreviations

AP	access point
BLE	Bluetooth Low Energy
Bps	bits per second
CW	Continuous Wave
DVR	Digital Video Recorder
FEC	forward error correction
HD	high definition
Hz	Hertz
IoT	Internet of Things
ISBE	International Society of Broadband Experts
K	Kelvin
LAN	Local Area Network
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power WAN
nDVR	Network DVR
NFC	Near Field Communications
OOK	On Off Keying
OTT	Over The Top
PAN	Personal Area Network
PMU	Power Management Unit
RF	Radio Frequency
RF ID	Radio Frequency Identification
RX	Receive
SCTE	Society of Cable Telecommunications Engineers
SOC	System On Chip
TX	Transmit
VEH	Vibration Energy Harvesting
WAN	Wide Area Network
WLAN	Wireless LAN

Bibliography & References

ANSI C63.5-2006: *American National Standard Electromagnetic Compatibility–Radiated Emission Measurements in Electromagnetic Interference (EMI) Control–Calibration of Antennas (9 kHz to 40 GHz)*; Institute of Electrical and Electronics Engineers

The ARRL Antenna Book, 20th Ed.; American Radio Relay League

Code of Federal Regulations, Title 47, Part 76

Reflections: Transmission Lines and Antennas, M. Walter Maxwell; American Radio Relay League