Bluetooth for IoT Deployments

Akash Malla
Santa Clara University
amalla1@scu.edu

Preface

This purpose of this paper is to discuss the enhancements in bluetooth technology via its flagship bluetooth 5 release, enhance BLE technology for IoT devices with addition of wake up radios.

Abstract

This paper gives an overview of how Bluetooth Low Energy (BLE) works which was introduced in Bluetooth v4 and how it can be enhanced to perform even better for large-scale IoT deployments. It is clear that bluetooth 5 has significant improvement in data upload speed and with an introduction of extended advertising mode for data transfer, it has the advantage from advertising mode with random access to advertisements and, on the other hand, dedicated data upload as in connection mode. Most of the users are using Bluetooth v4 right now and it is important to come up with some solutions that is compatible with that version as many devices do not support bluetooth 5 yet as it was recently released in December 2016. Also, when you use BLE alone in a large-scale IoT scenario such as a retail store, it would be communicating with lots of devices which would lead to contention and delays for data transfer. Therefore, this paper focuses on solutions on top of BLE such as Opportunistic listening, smart LaBLE system and Wake up Radios (WuR) in order to optimize BLE's performance.

Table of Contents

Table of Figures

1. Introduction

Day by day, we are seeing a huge number of IOT devices being used. According to Ericsson mobility report, by 2020 there will be 29 billion connected devices. In 2018, it is expected that IoT devices are going to surpass the number of mobile phones being used which explains the pace at which IoT devices are growing. The integral component of wireless IoT devices is radio interface which drains a lot of power. No matter which modern wireless transceiver is used for data transmission and beacon technologies, power consumption in listen mode on the devices when data is not being transmitted is an inevitable amount. The solution to unnecessary power wastage in order to connect wirelessly between devices is Bluetooth Low Energy (BLE).

For a while now, bluetooth has been used popularly to connect a mobile phone to a headset wirelessly. However, as part of bluetooth 4.0 release, BLE technology was introduced which opened up bluetooth to be incorporated by internet of things devices in the fitness, smart home and health industries. BLE provides the similar functionality as the older versions of bluetooth except for a much less energy consumption. When there is a pool of devices connected over the network, they have a common clock reference that appropriately reduces listening intervals and optimizes data exchange of each device. The devices connected over the network only wake up at a certain time to transmit data and at other times the listen mode is turned off which dramatically preserves heavy use of energy. Therefore, due to a server-client architecture and roles distributed asymmetrically for devices where the “peripheral” devices have limited set of responsibility and do not perform expensive computations done by “central” devices allowed effective use of power. Peripheral devices have data to be sent to central devices, this can be noticed in figure 1.

This paper will discuss the enhancements in bluetooth technology via its flagship bluetooth 5 release, how can BLE technology be improved with addition of wake up radios. It goes over smart solutions on how BLE could overcome dense IoT device areas and explains the advantages and disadvantages of Bluetooth 5 features such as connection modes, network and protocol optimization.

In chapter 2, three data transfer modes in Bluetooth 5 is explained along with a home automation use case which helps evaluate its performance for communication between IoT devices. Keeping in mind the great benefits of BLE technology, performance of bluetooth still has limitations when used for IoT devices, however, the latest release of bluetooth 5 has significant improvements. It has four times the communication range and twice the speed achieved compared to its predecessor. More communication range facilitates connection to IoT devices in many remote locations with good data exchange rates, along with other benefits like better throughput, low latency, and less time on air. This helps with battery life of the device due to coexistence of WiFi and other technologies that operate similarly to bluetooth. Other benefits of bluetooth 5 include 800% increase in broadcasting capacity like never before as this provides higher

adoption and usage of location-based services and beacons. Bluetooth is certified for two data transfer modes: connection-oriented and connectionless. Connection mode takes care of dedicating resources for data communication and connectionless mode, now called advertising mode, is data exchange over random access channels. The modification in connectionless mode being named as advertisement extension in bluetooth 5 release has additional channels for advertisements that was not there earlier.

Although bluetooth 5 feature enhancements propose a great use of it in the future, but since there are not many devices available with bluetooth 5 capabilities. Chapter 3 focuses on how BLE of Bluetooth version 4.2 could be enhanced to be energy efficient and provide fast data transfer capability through some modifications. First, BLE is explored and how it performances in dense amount of listening devices. Rather than actively scanning for devices at all times which costs energy, there is passive scanning. In passive scanning, there is an advertisement sent via an advertising channel and there is no response received whether the advertisement reached appropriate destination or not. In contrast, active scanning requires a direct connection where the sender should receive a response from the receiver to establish a connection. This chapter also discusses the benefits of opportunistic listening and Smart LaBLE system.

Chapter 4 takes a deep dive on how Wake-up Radios (WuR) help drastically reduce power consumption when used with BLE. A network of devices wake up at certain time periods to transmit data and later turn of their radio frequency in BLE standard. It uses common clock reference to keep track of when to turn radio frequency on/off. However, if common clock reference is down, the network of devices would stay active continuously to ensure it could receive data which leads to great energy consumption. So, in order to expect optimum power usage, latency and contact probability, research suggest to use new type of devices called Wake-up Radios. These radios allow almost no energy consumption when used without complex radio frequency modulations or management of payloads. These devices are most effective for listening mode to detect any incoming data payloads, rather than for actual data exchange itself due to their low sensitivity.

2. Data Transfer modes in Bluetooth 5

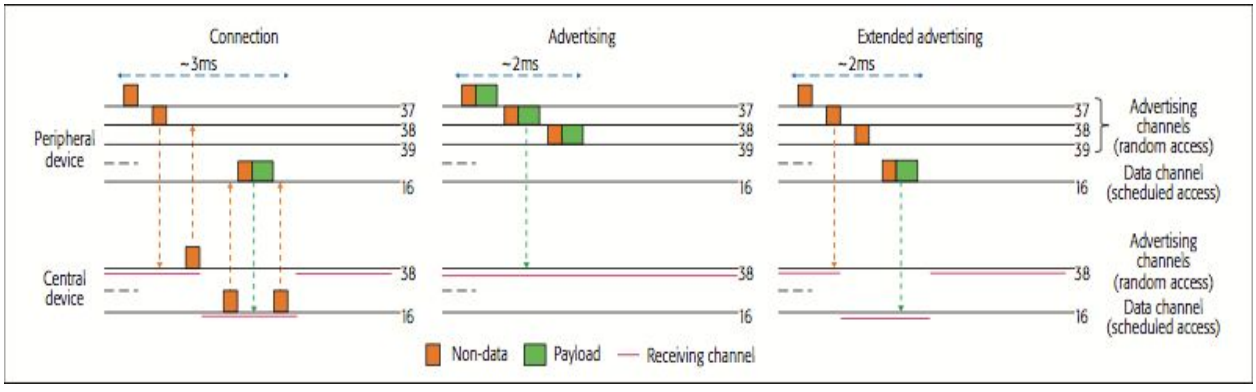


Figure 1: Three data transfer types/modes (Connection, Advertising and Extended Advertising) in Bluetooth 5

Channel access and data transfer operations are done through Bluetooth link layer. From a total of 40 physical channels, 37 channels are used for scheduled data transactions for exchange of data and the rest of them are used for random access advertising channels.

2.1 Connection Mode

As you can notice from Figure 1, in connection mode, each device establishes a connection for dedicated data transmission of packets. When a peripheral device wants to transmit some data, it sends a packet with no data to its intended destination periodically, the non-data packet is also known as connectable advertising packet. In response to this packet, the destination accepts the incoming request by sending a connection request to the same device. Alternatively, bluetooth 5 release can set up a connection over the newly developed physical layer data transfer mode. However, for the purpose of this paper, the older connection setup module is focused.

In an established connection, peripheral device stops advertising and data transmission begins between the two devices over a defined period of frequency hopping data channel. The period during two devices are communicating to each other over an established connection is called connection event. For every new connection event, a different channel is used for data transmission. When there is a channel noticed that has lot of frequency interference, it could be blacklisted such that connection events do not use this data channel. Bluetooth 5 has an enhanced pseudo-random sequencing scheme in order to do frequency hopping by ignoring any blacklisted frequency channels. The central device is responsible for the start and end of connection for data transmission. Once a connection is initiated, until acknowledged by the central device to be terminated sent from either of the two devices or a supervision timer comes to an end, connection stays active.

Bluetooth 5 consists of two ways to operate on network connection:

- Persistent connection: each device has continuous connection to all its destinations.
- Non-persistent connection: established on demand for each packet that needs to be transmitted.
- An application developer gets to choose which connection mode to use at the host layer by configuring some parameters.

In persistent connection, each node keeps an ongoing connection to its destinations. The connection is kept active by a connection event, where master send a message to its slave and the slave acknowledges the message.

- During a connection event when data is being transferred, there can be a wait time incurred as messages are transmitted across multiple nodes as in a mesh topology where the bluetooth link layer is used to combat this problem.
- When there is no connection event, the nodes goes to sleep which allows for a great energy utilization rather than devices listening or advertising all the time in an on-demand connection.

One of many complex problems with persistent type of network is how a device searches and creates a connection to the network. The way it joins the network leads to another common problem which is how to handle concurrent connections with a basic topology. Although there is no predefined standard that specifies how many concurrent connections would be supported, however, there has been limitations noticed on simultaneous connections each device can control. For example, nRF51822 is a popular nordic chipset that can support up to eight connections.

Since non-persistent connection is an on-demand connection it provides flexibility and scalability to huge networks. One problem with on-demand connection is that devices need to keep scanning advertising channel all the time which takes a significant toll on energy consumption. In addition to the problems, advertising channel congestion is prone in the network as the channel does not stop to set up more connections in such scenarios. However, accepting more connections and connections having a way of acknowledgement showcases reliability.

Bluetooth 5 supports IP-compatibility when operating in connection mode, however, not yet in connectionless mode. When there is high bandwidth for connections, it benefits in scheduled data channels, encryption and link layer acknowledgements, segmentation and reassembly given by higher-layer protocols. It supports multiple unicast packets in peer to peer separate connections as it does not support multicast.

2.2 Advertising Mode

Data payload is accessible across all three advertising channels so that devices scanning the advertising channel can retrieve the data by making a connection to one of those advertisements. In the center of figure 1, it illustrates how the data payload is available in all three advertising channels. Channel number 37 and 39 are non-connectable advertisements in figure 1.

The payload size in the advertising channels are limited to 27 bytes and 100ms of minimum interval time between non-connectable advertisements. Due to these restrictions, overall bandwidth availability is limited to some kilobits every second. Benefits of advertisements include absence of control message exchange requirement and multicast transmissions are accepted. However, there is no acknowledgement received from the device that receives the data and encryption is not standardized for packets in advertising channels.

2.3 Extended Advertising Mode

The extended advertising mode is newly introduced in Bluetooth 5 in order to take advantage of advertising at the same time use more channels for data transmission. You can see this mode being illustrated in the right side of figure 1.

Peripheral devices send short non-data extended advertisements in all three advertising channels, these channels can be represented as primary advertising

channels. There is a pointer to secondary advertising channel which is chosen at random from one of the extended advertisements. The receiver expects to receive data payload from a data channel that secondary advertising channel knows where this data channel is located at. Once primary channel is terminated after an advertising event, the data payload is transferred over the secondary advertising channel in a supplementary advertisement packet. Due to the ability of Bluetooth 5 devices to transmit data payload over secondary channel shows that it can scan the legacy three advertising channels as well as the secondary advertising channel.

Bluetooth 5 specifications does restrict the size of supplementary or auxiliary advertisement packet to be 251 bytes and a minimum interval between each advertising event set to 20ms. However, due to the need of transmitting advertisement packet from primary to secondary channel, the minimum interval could be longer to suffice for this basic advertising case.

2.4 Home Automation Use Case Scenario

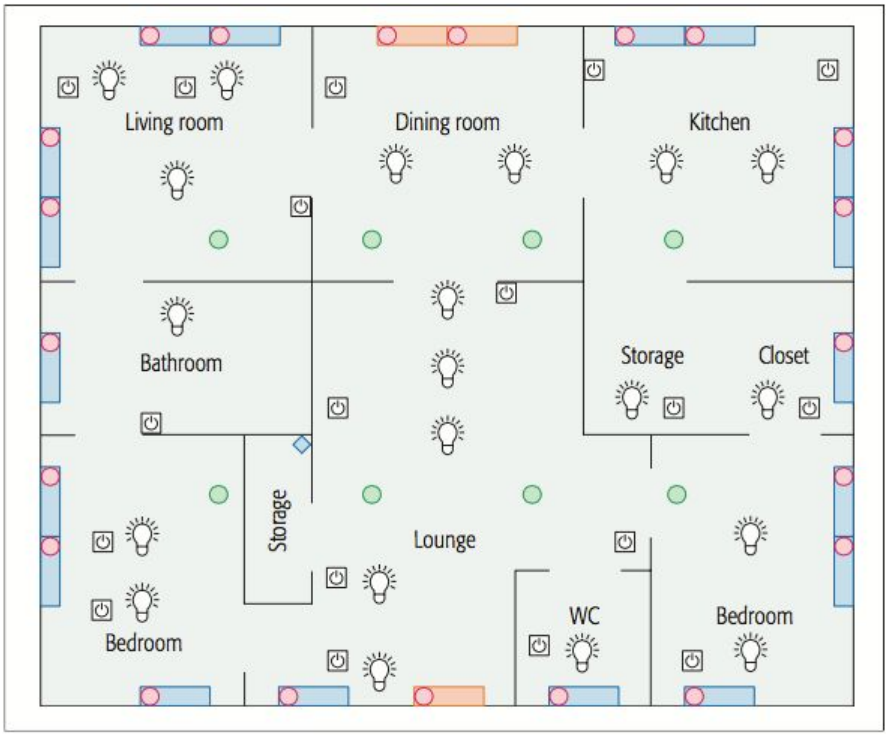


Figure 2: Home Automation simulation scenario.

One of the best use cases of bluetooth is automating home using IoT. Figure 2 depicts a single family home that has a measurement of 12m by 10m. IoT devices have been placed within or just outside the house. These devices would operate things in the house such as windows, temperature control, asset tags, light bulbs and switches. Overall there are 77 sensors and actuator devices placed in the house which includes a central gateway, in other words, a main bluetooth device.

The main bluetooth is always active with a radio receiver to communicate with IoT devices. It uses application logic to mimic a local cloud network of devices and it could connect to internet for sending messages to an external system.

Sensor devices in the house are almost always in sleep mode. Only during a sensor report, it requires each device's radio signal active for communication of data to the main bluetooth device. These devices conserve energy by being inactive except times when a sensor report needs to be generated that is triggered by the main bluetooth.

Actuator devices on the other hand, would not be able to conserve as much energy as sensor devices as they must be in constant communication to the main bluetooth to act on application-layer actuation commands. They must be always checking advertisement channel for any data sent from main bluetooth.

Radio signaling strength of the device is modeled using indoor propagation model, where there is a propagation loss of 6db to transmit signal through walls and 0.5db loss for every meter. Due to multipath propagation, we come across obstructions that result some fading channels. SNIR (signal-to-noise-and interference power ratio) determines the probability of data transmission to the receiver that is listening and tuned to proper channel. Also, it determines modulation performance at the physical layer and what coding scheme was used.

This model focuses on two kinds of messages sent from the application layer:

- Sensor report: This is sent from every sensor device to the main bluetooth as a message that contains statistics on physical property and notes changes in physical state. For example, it would have light switch is turned on or off, point of location, temperature changes. It is possible that a sensor report is sent with no respect to change in state in order for main bluetooth to confirm the device is responsive. Typically for security applications, if such messages are received then it determines that sender device is dysfunctional.
- Actuation command: Sent from main bluetooth to particular devices in response to a sensor report. For this example, an actuation command is sent only when for a light switch sensor report received.

Messages in application layer are randomly generated and it arrives in an exponentially distributed inter-arrival time. Below is a table that showcases each type of device and how often messages are present:

Types of Sensor Devices	Number of each type of sensor device	Send data/presence message every

Window Security Sensors	21	5 seconds
Temperature Sensors	8	60 seconds
Asset tags	10	1 second
Switches for light bulbs	18 switches, 20 bulbs	5 minutes

The data payload that is sent over the network is of size between 27 to 251 bytes. This range of size corresponds to the maximum capacity that a single advertisement can carry in the primary and secondary channel in order to use extended advertising connection mode. The application layer is straightforward with no complex higher-level protocols used.

2.5 Performance Evaluation

The performance of this network of devices is evaluated using three aspects which are as follows:

- Service Ratio: Generated traffic corresponds to all devices that are connected in the network, whereas severed traffic corresponds to whether data is being transmitted completely to the right destination or not. So this will consider uplink and downlink movement of data.
    - It is calculated by computing the quotient of severed and generated traffic. The traffic loss ratio is another metric which is a complement of service ratio.
- Packet Delay: This metric corresponds to the time taken from when a sensor report is sent to when an actuator command is received.
    - In this case, this metric measures for light bulbs. This measurement is for application layer only and processing time during a setup is ignored.
- Battery Lifetime: This metric measures time for a fully charged device to run out of battery and become completely dead.
    - It is computed assuming the devices have 220 mAh battery capacity, the battery is consumed for different states of the device. In active state it consumes about 10 mAh and in idle state about 1 uA.

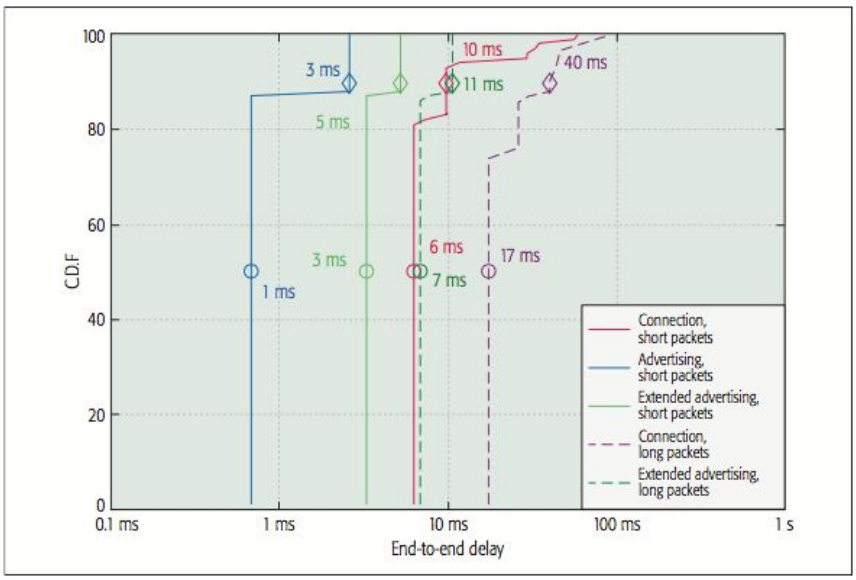
Figure 3: Generated Traffic and Traffic loss ratio of packets from size 27 to 251 bytes (service ratio).

The graphs in figure 3 show the performance and traffic generated by three data transfer modes. Short packets depict packets of size 27 bytes and long packets depict packets of size 251 bytes. One could notice that the short packets could be the only size used by legacy advertising channel, however, the extended advertising channel supported packets of size short and long. Comparatively, asset tags and window sensors had more traffic generated versus temperature sensors and light switches. In connection mode there is a tiny portion of data is lost which is ignored.

In terms of advertisement data messages, the loss of data is much higher and needs to be retransmitted. It is clear from the graph that extended advertising mode has the worst performance compared to other modes. The reason for that is while secondary channel is receiving data, other messages from main bluetooth cannot be received in extended advertising mode. Since the receiver is not available it results to a greater loss of data compared to advertising mode. In critical scenarios, for example, window sensor security, around 5-6% loss of data in the long packets will not be acceptable. Therefore, there will be few redundant packets seen in advertising events.

Figure 4: Shows Cumulative Distribution Function (C.D.F) for light bulb's end to end delay to receive short and long packets (packet delay).

The graph here depicts C.D.F for delay of receiving 27 and 251 byte payloads. As mentioned earlier, delay is computed for all successfully sent packets to the receiver.



When using legacy advertising channel for short packets, the shortest delay time is less than 1 ms. This is because there the payload is accessible in all three primary advertising channels for the receiver to randomly scan and transmit the payload.

At the top, for the advertising short packets, small portion of the payload is sent in 3 ms.

The additional time for that small portion is due to delay in sending actuator commands from main bluetooth device to the switches because sensor reports from switches were sent in sequential order. In terms of long packets perspective, extended advertising mode has the least delay time. Connection mode in general leads packets to have higher delay due to retransmission of packets for loss of data and supervision timeouts.

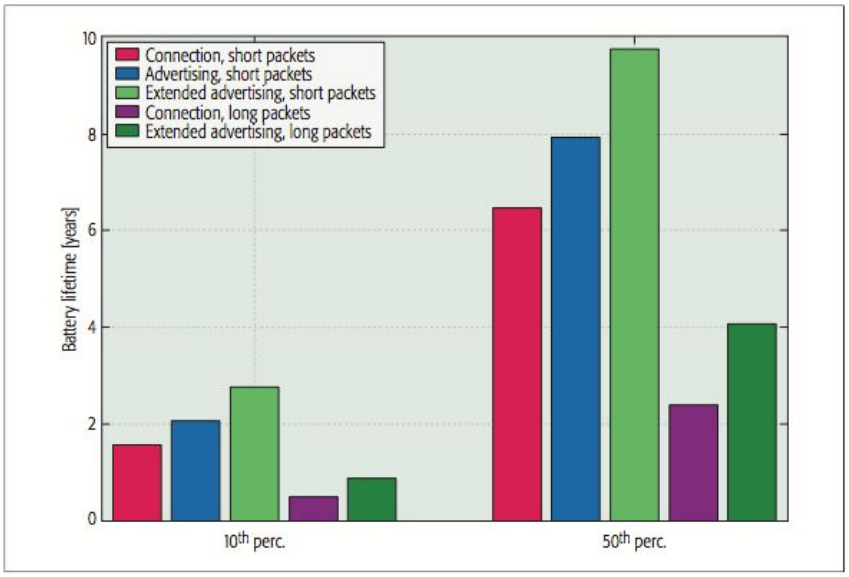


Figure 5: Sensor Device's battery life for short and long packets in different data transfer modes (battery lifetime).

From this graph, the important thing to notice is advertising mode has the longest battery life compared to any other connection modes. When comparing advertising and extended advertising mode, extended advertising mode has a significant difference in battery life because in advertising mode the devices need to keep scanning available advertisement for packets, whereas, extended advertisement mode allows to save on that power consumption. Lastly, in the short packet case, advertising mode beats connection mode as connection mode needs more power for retransmission of some packets.

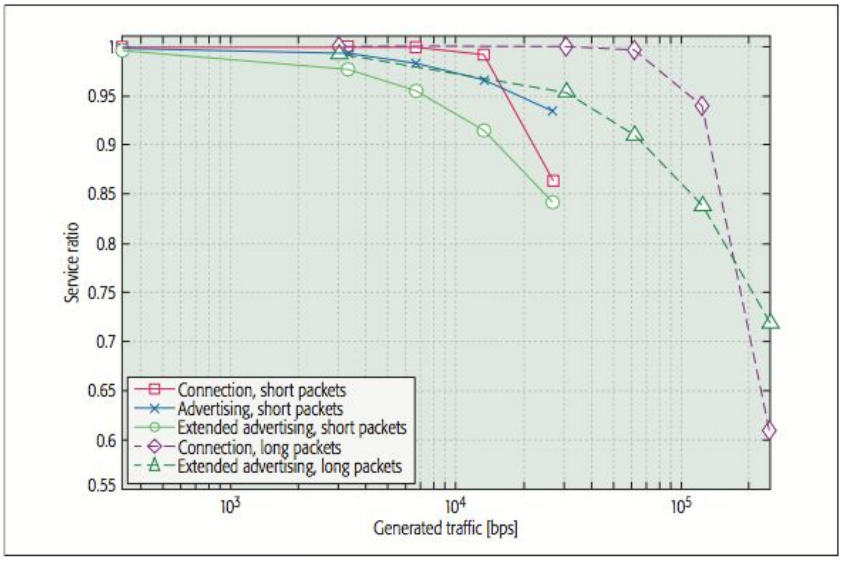


Figure 6: Service Ratio versus Generated Traffic for short and long packets

The graph in figure 6 allows us to understand

which data transfer mode is favorable as the traffic increases. For example, advertising mode is much more favorable than extended advertising mode when there is a high traffic of 27 byte or short packets. Similarly, for long packets or 251 byte packets, connection mode can handle lighter to normal traffic compared to extended advertising. However, you see an exponential drop in performance of connection mode when it needs to handle heavy to very heavy traffic, this is because of the connection timeouts which lead to multiple advertisement retransmissions.

3. Bluetooth Low Energy in Dense IoT Environments

Keeping aside the reason why BLE could be modified or enhanced to work well in dense IoT environment, there has been other ultra low power wireless technology solutions for short range communication. To name a few, near field communication (NFC), RFID, Bluetooth before BLE, and ZigBee. However, none of them have great potential to communicate with IoT devices in terms of cost effectiveness, availability and handling complex scenarios in an energy efficient way:

- Problem with NFC is it works only for very short distances which is roughly 2 inches. For example, if a user is walking around a bunch of products, NFC has a strong limitation to support such scenarios where it is common for IoT applications.
- RFID on the other hand has good range support, however, RFID is expensive for being embedded in devices.
- The classic bluetooth is quite available on almost all mobile phones nowadays, however, it still cannot handle IoT application's demand for complex discovery of surrounding devices.
- Lastly, ZigBee seems like a plausible solution for IoT as it can support good range communication and complexities of IoT applications. However, it is not being used in mobile devices limiting its usage in public deployment.

In consideration of all these limitations, BLE shines as the best solution so far in the IoT realm. BLE allows to handle the complexity of discovery of devices around the communication range and eliminate pairing which was there in classic bluetooth. Since it also supports short data transmissions, it pretty much full fills all the requirements of IoT combined with the fact that BLE could run on top of classic bluetooth chips which are available in many mobile devices. With the growing demand of IoT, experts believe BLE tags put in large spaces such as retail stores where there are tens and hundreds of products that could be advertised. Furthermore, there is a steady increase in the number of smartphones and other devices listening for data which will only make things more complex in future. That is why it is key to come up with solutions that build on top of the advantages of BLE to combat congestion of networks and collision of data packets being transmitted.

Although, everyone in general agrees the future of IoT deployments is on the rise, nobody bothered to prepare for the impact of communication for devices in dense IoT environments earlier. The contention period in BLE channel in dense environment scenarios will quickly become a blocker to handle the data traffic in high number of IoT

deployment areas. There are two main sources for conflicts, one is called by an increasing amount of devices to be scanned and the other is due to large-scale IoT environments for advertising data.

3.1 Bluetooth Low Energy

BLE was designed to use low-energy by reducing the scanning intervals of devices only when necessary and simplify and fasten data exchange. The way it works is first it sends an advertising message for a predefined period which is configure in the advertisement packet. In general the advertisement periods range from 100 ms to 1 s. Shorter advertisement periods for access to data to be faster could end up with more data packet conflicts ultimately causing more delay as the data packet would need to be sent again.

BLE separates actual data upload via a connected communication from just sending advertising messages. As mentioned in earlier chapter, there are three available advertising channels to send advertisements. Keeping only one advertising channel would cause for congestion when sending advertisements and at the same time having too many advertising channels would take away bandwidth which could have been used for data transmission and lead to slower access to advertising messages. These channels do not overlap with 802.11 or WiFi frequencies allowing bluetooth to co-exist with other wireless technologies like WiFi.

BLE has a periodic advertisement protocol where at the beginning of an advertising interval, an advertisement message is sent over each of the advertising channels. Listening devices scan for advertisement messages by going through each channel. The action taken by the listening device is determined by the kind of advertising message: active or passive. No matter what type of advertising message, the scanning period promises to capture an advertising message at least one time over advertising interval with no conflict or loss of data.

As multiple BLEs could send an advertising message in same advertising channel within one advertising interval, each BLE adds 10 μs of buffer to its advertising packet to avoid possibility of a collision if a collision has already occurred. This additional buffer to each BLE's message especially helps to reduce conflict drastically when overlapping transmission happens in same advertising interval. Also, provided that the advertising messages are quite small, with this additional buffer, this approach can significantly avoid collisions when there are large-scale IoT deployments of around 200 or more BLE tagged devices in communication range.

In order to maintain energy efficiency, the BLE tags are active for short intervals in order to send the advertising message. Energy consumption is further conserved by turning off carrier sensing from media access control (MAC) layer in BLE. In order to conserve this energy, it comes with a cost of increasing the chances of potential contention.

There are two basic operations that BLE can do:

- Passive mode: ability to send data payload up to 31 bytes.

- Active mode: in order to advertise data more than 31 bytes.
- BLE listening device that receives passive advertising message follows passive advertising rules, similarly, when listening devices receive active advertising message then they follow active advertising rules.

3.2 Passive Scanning

Passive scanning is the simplest message mode in BLE, in this case, each device sends a passive advertising message to each of the advertisement channels. The size of the data payload is restricted to up to 31 bytes and up to 10 ms wait time between each transmission of advertisement messages. However, typically these messages are sent right after one another on the three advertising channels. There is no direct connection between the advertising channel and the receiver as the receiver is just listening to the advertising message.

3.3 Active Scanning

Some applications require to send more than 31 byte of data payload, in that case an active advertising message is sent to the advertising channel. The active advertising message calls for a three-way connection. All listening devices that are receiving this advertising message respond with a scan request to the advertiser, the request has a unicast to the BLE. The advertiser or BLE completes data upload with a scan response. This response could contain an additional 31 byte worth of data which doubles the data payload capacity which was available in passive scanning. The response is broadcasted to all potential advertisers.

This three way advertise-request-response process is done very quickly, most of the energy consumption lies on scan request and scan response sent. BLE tags are required to wait for a minimum interval of time to see whether scan request was sent or not after advertising message. Even though as per BLE specifications channels can have wait time of up to 10 ms, tags do not wait long enough to check for a response received. Once the first scan request is sent over a advertising interval, tags respond just once on each advertising channel.

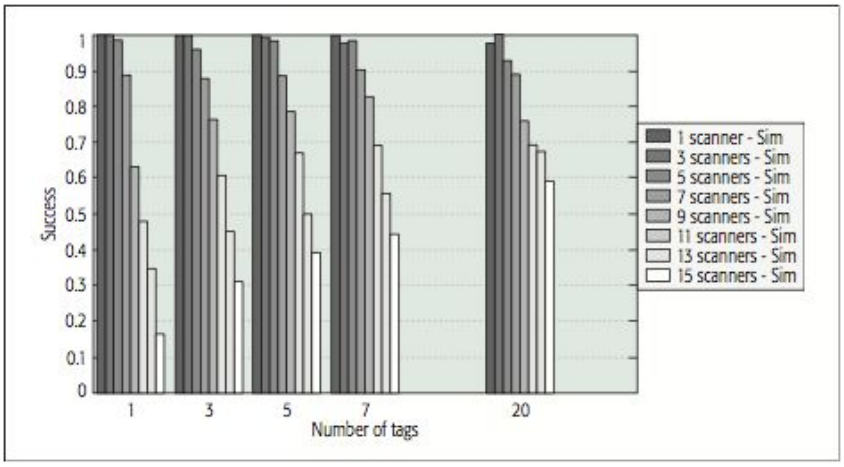


Figure 7: Shows the success rate for data transfer with different number of BLE tags.

Even though, scan response is a broadcast to all listening devices, only the requested BLE tag is supposed to act on the response assuming the same BLE tag is within the advertising interval in the channel. Otherwise, non-request scan responses are discarded. So, if any device receives a scan response before it triggers a scan request, that scan response is discarded. When this happens, it delays the process as the scan request would be triggered as part of the next advertising period.

The conflict problem related to active scanning is listening devices. The dispatch of scan request message is similar to sending an advertisement message because it does not include carrier sensing. However, these are the main problems:

- Basically when there are lots of incoming advertising messages from the advertising channel, the result is a bombard of scan responses to BLE tag. This way most of the requests are lost.
- Listening devices could add a buffer to protect against collision, however that is of minimal help. There are two drawbacks from this approach:
    - Firstly, more wait time for advertising messages to flow in the advertising channels, which affects more energy consumption as the BLE tags stay active until it receives a response from listening device in the advertising interval.
    - Secondly, the buffer need to be long enough to promise no collisions as there is no carrier sensing. However, this leads again to longer time BLE tag is active rather than being in low-power mode.

Because the scan response is broadcasted, all BLE tags could be able to see and access the response messages. In such a open wireless network, a broadcast of large number of scan requests could end up with no request properly processed by the BLE tag. If no request is properly received to the advertising tag then no response message is fired.

Backoff mechanism is used in order to get around conflicts during scan request messages sent. This mechanism implemented at the listening device, comes with its own set of drawbacks. Backoff allows to stop wasting energy in the next advertising period where it helps stop any nearby scanning devices preparing to send out a request with additional data packet because in the current period, a tag does not get its response. This way, the nearby listening devices choose to backoff in the next period to bypass any collisions. It is possible that some listening devices could successfully trigger a request while in a backoff state, however, the response to that request is not accepted by those listening devices.

3.4 Active Scanning Performance

The number of scan response messages accepted provides data for successful run in active scanning to understand performance of BLE. First of all, as mentioned

earlier, BLE tag must send an advertising message so that a scan request is sent from the listening device is captured at the BLE tag.

Just by looking at how many loss of response does not provide good enough metric to asses an IoT environment. In fact, lots of IoT applications that have human intervention are fine with some delay. For example, a loss of data would not be much noticed by a person as long as the data is received within a time interval. Therefore, a more valuable metric would be to calculate how much success in receiving data packets within a given time window. Let's say the advertising interval is set to 1 second. Users could generally expect the result shown in 5 seconds. This means response message has been successfully received from a scanning device within 5 seconds of the request to at least one of the BLE tags. For successful request and response message received within 5 second window is called total success.

3.4.1 Simulation Analysis

To understand how much BLE is impacted by the density of radio activity, the experiment involves looking at success rates when there is a range of odd number of scanning devices from 1 to a maximum of 15 that were listening for 1,3,5,7,9,20 and 50 advertising messages.

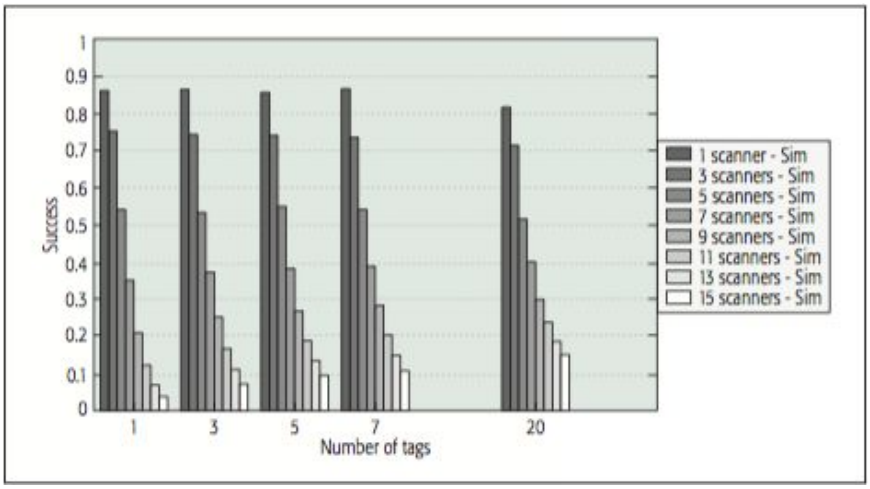


Figure 8: Total success rate for various number of scanning devices (n3 simulation).

From the graph in figure 12, total success only reaches up to 85% when the number of scanning devices are 1 and 3. However from figure 11, 5 second success rate is pretty much 100% no matter what the number of scanning devices were. Basically, when scanning devices are allowed to wait, it causes for loss of success rate.

Due to having three advertising channels, it causes the rapid success rate decrease in the graph from figure 8. Even though the scanning devices are not communicating with each other to be synchronized, having three advertising channels causes some channels to carry more load than others for the request and response messages. When you have only 1 scanning device, it would choose a channel to scan and no collisions would be expected. When you have 5 scanning devices, in that case,

there is still a chance that only one of the devices sends a request. However, when there are 9 scanning devices, success rate drops drastically due to high contention.

As the number of listening or scanning devices increases success rate proportionally drops. However, success rate is very low for very less number of listening devices too. The reason is if say only 1 listening device is there, success rate fully depends on this device. It is possible that multiple listening devices are simultaneously trying to retrieve data from same device. Once there are 10 or more listening devices, no matter what scenario, the success rate stays in the range between 60-70%.

3.5 Opportunistic Listening

From the analysis done on BLE, it is understood that contention and backoff are causing for the dip in success rate with scanning devices. Backoff period does not allow for the scanning response to be accepted by the requester and causes for delay and response to be removed. And as seen earlier, chances of contention increases as more listening devices increases. As a workaround for these two problems, opportunistic listening allows the non-requested scanning response to be accepted during backoff period. If there is at least one scanning device that sent a scan request message, then the scan response message are still accepted and acted on by all scanning devices that are in backoff mode. One thing to note is opportunistic listening will only accept and process scan response messages when requester sent a scan request during the time backoff period was not enabled. Any unrequested scan responses are discarded according to BLE specification to conserve energy from accepting such messages.

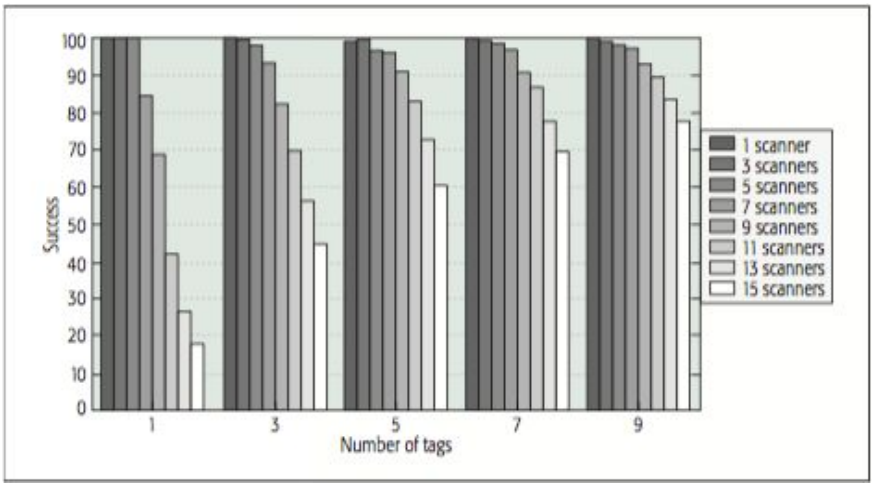


Figure 9: 5 second success rate for scanning devices using opportunistic listening

As per expectation, opportunistic listening allows much better accuracy by the acceptance of response messages for requests that was sent before backoff period. Notice that as more scanning devices are added, the success rate is increasing due to its cooperative nature. However, for a single BLE tag, when the number of scanners increase, success rate is down dramatically. The reason is too many scanning devices are communicating with the single tag leading to heavy contention. Thus, for large-scale IoT deployments such as retail stores, a more optimized solution is required.

3.6 Smart LaBLE System

Essentially, smart LaBLE provides a way to avoid contention by having multiple objects advertise the same data. Consider a retail environment, where each product needs to be advertised to all shoppers to educate them about the product and possibly help them decide to purchase that item. Another use case is each product needs to be tracked for management purpose in the store too. Smart LaBLE system would help in this case to advertise the product information nearest to the product. It can dynamically show the product information depending on the products that are in the shelves, so if the products end up being moved somewhere else in the store, Smart LaBLE would automatically display the right product information that is on a shelf and also provide the number of each type of product on shelf. This will work as long as the distance between Smart LaBLE is less than two times the distance between one product type to another product type. It uses received signal strength indication (RSSI) value to calculate and display the right product information near it.

4. Bluetooth Low Energy with Wake up Radio

A network of devices make use of a common clock reference in order to have efficient listening intervals for devices to save on power consumption. The Bluetooth Low Energy (BLE) standard allows for a network of devices to wake up at certain time periods to transmit data and later turn of their radio frequency, however, what would happen if the common clock reference device goes down? This would cause major problem as devices would not know when to turn on and off to transmit data. As a worst case scenario, the network of devices would stay active continuously to ensure it could receive data. The power needed for devices to always be active would cost more than the actual transmission of data. There are specific MAC protocols that could analyze the activity between transmitter and receiver to reduce the total activation time. However, we cannot expect optimum power usage, latency and contact probability using a MAC protocol.

To overcome the problems stated earlier, research suggest to use new type of devices called Wake-up Radios (WuR). These radios allow almost no energy consumption when used without complex radio frequency modulations or management of payloads. These devices are most effective for listening mode to detect any incoming data payloads, rather than for actual data exchange itself due to their low sensitivity. Therefore, WuR will help dramatically reduce energy usage that would have gone wasted by having all devices to be idly listening or scanning, whereas WuR can not only listen in a much more efficient way but also keep main radio turned off until needed. Although there have been experiments and research proving its great benefits, there is no standard protocols to use WuR and so has not been integrated along with BLE. Ideally, integrating WuR and BLE to be used for IoT application is a futuristic approach to solve all the current problems being faced using just BLE or even using latest bluetooth 5 technology. The emerging IoT deals with interaction between a huge number of devices which in turn increases the probability in loss of data through packet collisions. The time needed for a device to get in touch with a channel in a dense network of devices and network latency, would not be a considerably big problem with this new approach.

4.1 Approaches and Challenges of WuR

Asynchronous activation of wireless sensor devices has been a popular study in the research community. As part of that research, here is a list of some approaches:

- Out of band (OOB) communication, where there is no use of light or sound, in other words, no radio frequency (RF) medium. Although very effective for some applications, this approach is not applicable for all types of applications as surrounding environment and noise could limit its capability.
- Use of WuR with RF where there is a dedicated band for the main radio signaling. It resolves problems with OOB approach regarding environment, however, OOB with RF communication would require additional hardware for wake up signal. To combat the problem to require more hardware, there has been some in-band solutions which would use existing main radio's hardware on some IoT devices.
- WuRs for Body Area Networks (BANs) is another area of research as BAN communication involves less distance, typically few meters, to make WuR effective and dependable.

To utilize the full potential of WuR, the model should have a low power receiver in combination with a standard protocol. However, it is still at the early stages of development and research where the standard protocol for WuR is not yet properly available making it difficult to have these new class of receiver devices with prominently used standards such as BLE. The best implementation known so far is a low energy wake up trigger to turn on devices whenever needed.

Studies show that BLE integration with WuR has been attempted. The model consists of hardware design and standard protocol to signal WuR devices, however, it is not fully tested hardware with respect to scalability. This implementation uses Code Division Multiple Access (CDMA) modulation method for hardware to offer device-dependent WuR trigger. Once signal is detected by receiver, the signal is processed in a baseband processor where depending on power used and time-based pattern related to BLE advertising packets sequence, this determines whether the signal message is to wake up a device. The performance of CMOS based hardware reaches power consumption of 236 nW and sensitivity of -56.5 dBm, this is quite impressive numbers.

Wearable devices and for short range communication, BLE technology has been prominently used standard, however, there are noticeable limitations to consider. One of two main limitations in advertising mode are packet size and absence of time taken for packet transmission.

Since the focus is on IoT applications, BLE beacon is a way for bluetooth enabled devices to find out location and based on the environment and proximity of the device, it could provide some services. Especially in densely populated areas, where there are hundreds of BLE beacons in range for communication, this is the scenario IoT applications should fundamentally be able to handle and scale.

In order to analyze IoT application, a simulator has been developed to mimic multiple BLE radio frequencies in the two main data transfer events: advertising event and connection event and request. This simulator assumes medium access to BLE devices for a real world scenario. When the radioactivity is in play, there will be collisions

and connection request failures that would be detected by the simulator. BLE events consist of many TX and RX transaction phases on various channels, however, for the purposes of this simulation, TX and RX are focused only on one advertising channel. Simulation results are still trustworthy because a receiver cannot scan multiple channels at a time and connection packets and advertising packets are dispatched on different channels. Therefore, as there cannot be two connection events active at a time, collisions cannot be possible when considering to focus on one advertising channel.

Here are certain rules followed in the simulation experiment:

- All experiments are simulated by using N number of beacons and all of them are configured exactly same.
- All beacons use same advertising interval (T_{ADV}) and always full fill BLE packets.
- Below are different types of BLE packets and its specifications:
    - Advertising packets are of size 47 bytes (with 31 bytes of data payload).
    - Connection packets are of size 41 bytes (with 20 bytes of data payload).
    - Connection requests are of size 44 bytes (only configuration data).
- Bluetooth v4.2 is used for this experiment and it uses 1 Mbps for modulation, for example, a 47 byte packet would take 376 μs.
- The BLE main device has reciever always turned on and it can perform following actions
    - Beacon discovery
    - Can connect to a beacon one at a time
    - Exchange data using BLE connection scheme.
- Simulator starts all N beacons and assigns them to an ideal advertising interval (T_{ADV}).
- A random initial offset is set for the following range for each beacon: [0;T_{ADV}] after that each beacon starts to transmit advertising packet.
- After each packet is received by receiver in T_{ADV} + δ, where δ represents random delay in a BLE transmission, it is uniformly distributed in the following interval: [0;10 ms].

As per the above rules, once the central device starts to receive advertising packets successfully from a beacon, then that beacon is marked as discovered. If the advertising packets are overlapped, that means a collision occurred and the packet is not accepted by the beacon that sent it and it continues to scan for other packets. When there is a need for a connection to be established between the central device and beacon, right after a beacon is discovered, the central device sends a connection request to the beacon. There is a possibility that the connection request is corrupted as advertising packets and connection requests are transmitted over the same channel. If they collide each other, connection request is discarded as the beacon receives an invalid data.

The goal of this simulation is to find out time for the central device to discover all beacons that are available in the given area for a given N beacons and T_{ADV} advertising

interval. In order to have consistent data, all reports found have been averaged after doing 200 randomly independent tests.

4.2 Analysis of Bluetooth with Beacon

Provided that the simulator knows number of beacons and advertising interval values, it will help evaluate how much time it takes to:

- Discover all beacons
- Discover a beacon and send a data packet to it.

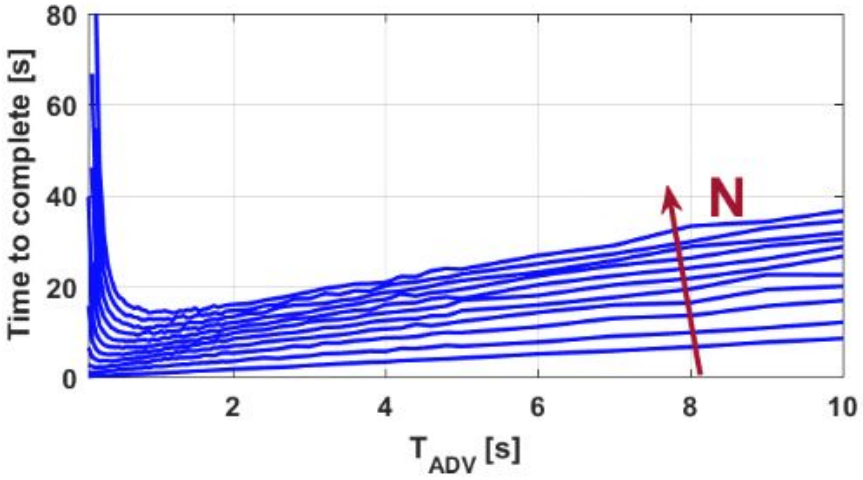


Figure 10: Average time to discover all N beacon nodes.

Every line in the graph in figure 7 represents the time to discover the beacons for different numbers of N in the y-axis versus advertising interval in seconds in x-axis. Advertising interval means the time taken between two advertising packet dispatched. N keeps increasing in the direction of red arrow as N grows from 5, 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000 beacons.

Advertising interval and colliding packets are two main influencers for representing discovery time. When there are less collisions, in other words, longer advertising intervals, discovery time is almost proportional to advertising interval and number of beacons. This is true because when a packet needs to be resent due to collision, same beacon will wait for T_{ADV} time. So, long intervals equal long time to wait for the packets to be received. Furthermore, if N is bigger number, then there will be more beacons to discover by the central device and so more collisions are possible. When we look at short advertising intervals, packet collisions are more frequent in crowded areas. That is why smaller advertising intervals lead to more collisions which then leads to central device to receive high corrupted packets that need to be sent again by the beacons.

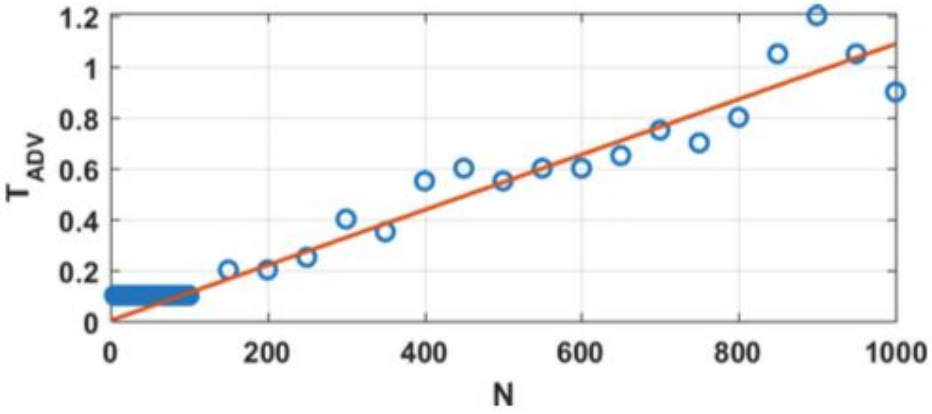


Figure 11: Optimal time to for the central device to communicate with all beacons for a range of N value. This graph represents the minimum time to discover N beacons from figure one with a best fit line plotted.

From figure 8, due to advertising interval and packet collision trends, the graph determines the ideal time for discovery of beacons. This data guides to set advertising interval given the number of beacons in reach for communication. Interestingly enough, for 1000 beacons the optimal advertising interval is close to 1 second and 53% of packets received to the central device had to be retransmitted due to collision. From the graph, there is a simple equation that could be come up where advertising interval is approximately equal to N ms. So, the following equation is true, where T_{ADV} = N ms, with around 53% of packets that would be corrupted and needs to be retransmitted.

4.2.1 Data Exchange

Aggressive duty cycle scheme is used by beacons in order to extend battery life and limit maintenance effort. As the beacons only transmit short packets in a predefined time frame, they activate radioactivity for strict timeslots for being able to transmit the packet. Until the next dispatch of packet, they remain in sleep mode. This way beacons conserve energy with low work cycles, for example from 1% of energy consumption to 0.01% that leads to an average energy consumption that is less than 10 μA.

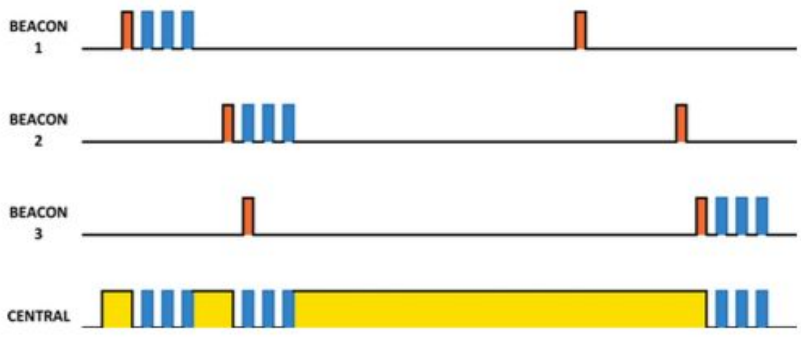


Figure 12a: This demonstrates the way in which the central device sends data to three beacons.

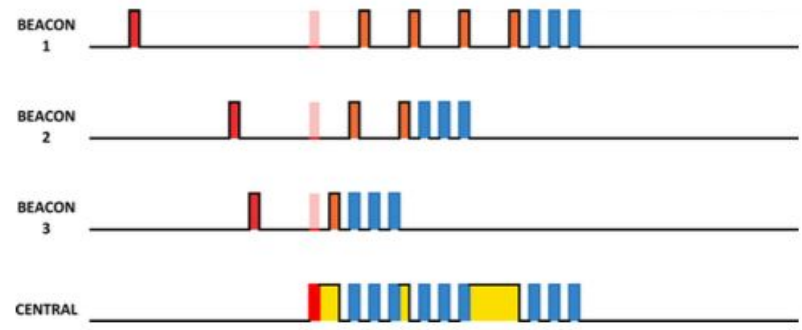


Figure 12b: Demonstrates connection oriented data exchange, where data is sent to three beacons using a wake up radio.

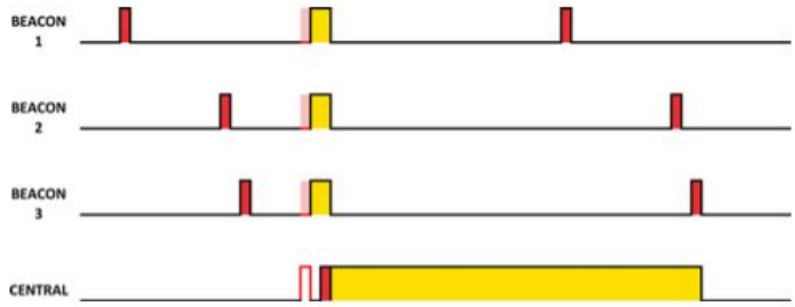


Figure 12c: Demonstrates broadcast oriented data exchange where each beacon receives same data from central device.

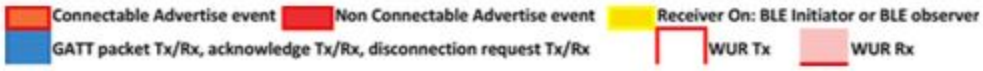


Figure 12d: Describes what each symbol means in figures 12a, 12b, 12c

In order to achieve a high efficiency in power consumption, the beacons do not scan for any incoming data. However, the beacon devices do need to retrieve data at some point for central device to send updates. To do so, it needs to be configured as connectable such that only then it will scan for incoming data in short span of time. Once connection between beacon and central device is established no other beacon can communicate with central device during that time. For example, by using 2 connection events a 20 byte data packet could be sent to beacon. First connection event is to send the data and the other is to send ACK (acknowledgement) that the data has been received and to disconnect the connection. This process is seen in figure 9a.

In figure 9a, once a beacon is in a connectable mode for advertising event and when central device is not uploading data to another beacon at that time and it has receiver on mode, the central device chooses to send data to that particular beacon. Therefore, BLE standard provides a way for beacon to activate central device's receiver to be turned on for connection request and data to be transmitted. However, what if same data needs to be sent to all beacons, it would be inefficient to use just BLE

standard in this case. So, BLE standard along with the use of WuR is shown in figures 9b and 9c.

WuR is an additional hardware that could be attached on all beacons, it would give the capability to trigger BLE embedded in the beacon devices when central device is sends a message, for example, on/off key (OOK) modulation. WuR does not support for correct addressing, however, that is not a problem as BLE does have that capability for a reliable addressing. There are several ways in which WuR has been implemented before that would not fit BLE use case. For example, when multiple devices are sharing a WuR band, it causes false wake up triggers hindering any improvements by the use of WuR.

In this case, WuR has been utilized for two different ways of data exchange: connection oriented and broadcast oriented. Connection oriented responds differently to wake up triggers than broadcast oriented. If the beacons cannot tell the difference in wake up requests from one to another, flexibility of this solution would be decreased. To solve this problem, wake up request should be set up in such a way that there is a clear distinction between two wake up calls.

4.2.1.1 Connection Oriented Data Exchange

This method is required to be used when there needs to be sent a specific data packet for a specific beacon. BLE connection is compulsory for this scenario as mentioned earlier WuR has no way to address a beacon. However, including WuR to each beacon helps improve the speed of the data exchange. From Figure 9a, beacon device broadcasts a connectable advertisement to central device, which corresponds to higher power usage, 30% more power than non-connectable set up, as the central device needs to respond with connection request and time slot sent to beacon.

Instead of using connectable advertising, a non-connectable advertisement sent to central device is configured for beacon. Using a different advertising interval, WuR then triggers the advertisement to become connectable. Once it is connectable again, the central device could connect using connection request and transmit data as explained earlier. As soon as the data is transmitted and disconnected from central device, for a predefined interval beacon stops advertising. By this way, there is an increase in number of beacons to which data is transmitted, at the same time, central device is not congested as there would be less beacons that are advertising.

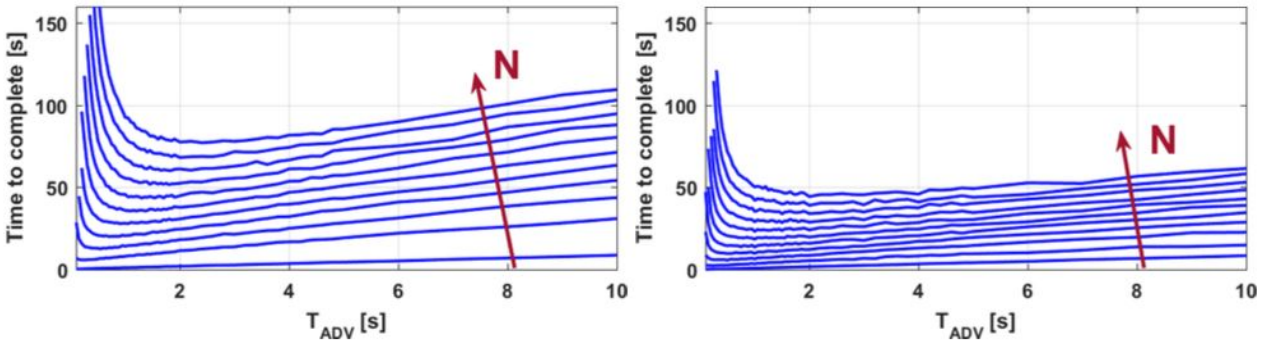


Figure 13: The two graphs shows the time to discover all beacons by sending 1 data packet to each beacon. Graph on the left is performance shown for BLE and on the right BLE with WuR. As you can see BLE with WuR is faster to send at least one data packet to all beacons compared to BLE. The positions of the minimum time to complete comparatively has decreased by 40% for the graph on the right versus the left.

Advertising interval is optimized in two phases of the process when using BLE with WuR.

- Firstly, a non-connectable advertising is used instead of connectable advertising for each beacon and then advertising interval is set.
- Secondly, WuR triggers to use connectable advertising for each beacon and advertising interval is set.

The use of WuR reduces total energy use by 30% because when WuR trigger call is done with virtually no energy use at all. Due to the optimum advertising interval setting with the use of WuR, if a beacon needs to retrieve data upload, then a longer advertising interval must be used to avoid congestion and conflicts in connection requests from central device. Therefore, the ideal advertising interval now is supposed to be T_{ADV} = 3N ms.

4.2.1.2 Broadcast Oriented Data Exchange

This method of data exchange allows when at times same data needs to be sent to all beacons from the central device. In such cases, WuR allows to simultaneously upload data to all beacons at once. This way helps reduce power consumption even more especially when data needs to be transmitted for a high number of beacons.

The solution for this data exchange works inversely where beacon acts like central device and vice versa. So, beacon's job is BLE observer, in other words, broadcast receiver, whereas central device's job is advertiser, in other words, broadcast dispatcher. With this configuration, all beacons get to receive same broadcast data packet from central device without establishing a connection to each beacon and sending same packets individually. This is shown in figure 9c.

As an assurance that all beacons have received the data packet from the central device, after the data transmission finishes to all beacons, the next time each beacon sends an advertisement packet, it includes an acknowledgement that is sent to the central device. The acknowledgement consists of a packet number of the last data upload in the advertisement packet. If this ACK is not sent the whole data upload process to beacons is just a little faster. Since the broadcast dispatch takes less than 1 ms, the complete time for discovery of beacons is what dominates more than the time taken for sending an ACK. Therefore, the total time taken for sending a broadcast packet and getting a ACK response from each beacon is equal to the time taken for just sending a broadcast packet to each and every beacon in the network.

5. Conclusion

In conclusion, there is a clear indication that the number of IoT deployments are bound to be used in almost all fields of work. When there is a need for an energy efficient and fast communication solution to operate with the IoT devices, bluetooth low energy is a great solution. However, there are multiple problems with classic bluetooth which did not have as much capability as much as what Bluetooth v4.2 with BLE has which proved to be efficient and workable solution for some IoT applications. Once BLE related problems have been exposed, many solutions are available to combat those challenges. This paper talks about the use of other pieces of hardwares such as Wake up Radios or just enhancing BLE by updating its core methodologies or addition of new methods, for example, bluetooth 5 introduced extended advertising mode.

Firstly in this paper, Bluetooth 5 has been explored in terms of what it has to offer:

- Faster than earlier: data transfer can complete in half the time than before at the same time with a widened data broadcasting range up 800%
- Longer range availability: range is increased 4 times more than Bluetooth 4.2 version allowing users to access service farther away without any disruption.
- Ready for IoT deployments especially due to the earlier point as the broadcast area is much more bigger allowing bluetooth to operate on IoT devices.

Next, BLE is explained in detail and below are the two solutions proposed as a way to improve its performance:

- One solution is called opportunistic listening which mainly resolves the problem to handle scanning for messages in dense IoT deployments. It does so by ensuring in backoff mode, the response messages are not disposed but rather accepted if a corresponding request message was sent by the scanning device.
- The other solution resolves a problem that opportunistic listening was not able to resolve which is performance degradation with the increase in scanning devices. Smart LaBLE system addresses for large-scale IoT deployment scenarios where there are a lot of passive scanning devices by pushing some of the detection work to scanning device.

Lastly, Bluetooth along with the use of Wake up Radios shows great performance benefits. The main reason is WuR consumes nearly zero power usage when used as a trigger to turn on or turn off a device. WuR does not have capability to handle complex RF and data exchange process which is taken care by BLE. Here is a summary of power consumption and time reduced using data exchange with beacons or scanning devices and WuR:

- 30% reduction of energy when beacons used non-connectable advertisements by taking advantage of WuR trigger.
- 60% or more reduced time for data upload process when using BLE connection as explained at the beginning of data exchange section.
- The above time reduction indirectly helps the central device 60% more energy efficient as its consumption is proportional to the time its receiver is on. However, central device is not as much of concern than the beacons itself because central device generally has less power restrictions.

6. Acronyms

ACK - Acknowledgement
BLE - Bluetooth Low Energy
CDMA - Code Division Multiple Access
CMOS - Complementary Metal-Oxide Semiconductor
IoT - Internet Of Things
MAC - Media Access Control
RF - Radio Frequency
RSSI - received signal strength indication
OOK - On/Off Key modulation
WuR - Wake up Radio(s)
T_{ADV} - Advertising interval

7. Bibliography

1. Harris III, A., Khanna, V., Tuncay, G., Want, R. and Kravets, R. “Bluetooth Low Energy in Dense IoT Environments”, *IEEE Communications Magazine*, pp.30-36, 2016.
2. Giovanelli, D., et al. “Enhancing Bluetooth Low Energy with Wake-up Radios for IoT Applications.” *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017, doi:10.1109/iwcmc.2017.7986527.
3. Partha Pratim Ray, Sneha Agarwal. "Bluetooth 5 and Internet of Things: Potential and architecture", *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) on*, pp. 1461-1465, 2017.
4. Piergiuseppe Di Marco, Per Skillermark, Anna Larmo, Pontus Arvidson, and Roman Chirikov, “Performance Evaluation of the Data Transfer Modes in Bluetooth 5”, *IEEE Communications Standards Magazine,* pp.92-97, 2017.