International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Presence Detection with Bluetooth Low Energy: A Review and Experiment

Kevin Jaglal [a], Michael Hosein[*b]

[a,b] *Department of Computing and Information Technology, University of the West Indies, St. Augustine, Trinidad*

[b] *Email: mhosein2006@gmail.com*

Abstract

Bluetooth is one of the most ubiquitous technologies in smart phone today and its prominence in other devices is rising rapidly. It has become the De Facto technology used when there is need for device-to-device communication. However, the evolving standard has much more to offer. Bluetooth can power many applications due to capabilities. A key metric of Bluetooth is the Received Signal Strength Indicator (RSSI) and depending on the readings one can infer locality. This study evaluates existing research that attempts localization implemented using the Bluetooth protocol and the metrics that power those applications. A proof-of-concept software is developed to further investigate the feasibility of presence detection using Bluetooth Low Energy without connection to a device.

Keywords: Bluetooth; Bluetooth Low Energy; BLE; Presence Detection; Localization.

1. Introduction

In today's society, productivity is shifting from working at just a desk but on the go with different classes of mobile productivity devices, be it laptops, tablets, sub-categories of each and even mobile phones. Thus, there is need to prevent unauthorized access to these devices either to protect company and personal data or just guard sensitive data and prevent unwanted use. Devices can be augmented detect and protect usage via fingerprint scanners and facial recognition. Capacitive Fingerprint scanners commonly found on mobile devices and laptops are great for authentication, but placement of scanners can be inconvenient or if the device is left for a moment unattended, someone else can use the device which has already authenticated now, a non-present user and it may be stolen and authentication mechanisms be changed.

---

* Corresponding author.

Similarly, these devices may have a front facing camera that may be able to provide facial recognition authentication either by taking a picture and analyzing the image or extra dedicated hardware for further analysis for authentication. Either way a commonality with these devices is that once authenticated, if someone else gains access, they can extract data or even disable device authentication procedures because the device remained authenticated.

1.1. Objectives of the Study

The goal of this work involves different types of Bluetooth hardware and attempts to achieve the following objectives:

By the review of literature, to investigate the current status of Bluetooth Technology in relation to localization and the metrics and features that allows for the highlighted need in functionality and to discern whether presence detection capabilities are feasible. Following that, develop a lightweight and user-friendly application that estimates if the user is in close proximity to a Bluetooth device, using existing consumer-based Bluetooth devices to lock the device within a reasonable range. Thus, implementing presence detection via Bluetooth. This experimental attempt will either align with the existing literature or prove against it. As of writing, existing measures depends on Bluetooth connectivity being dropped completely to make decisive action for Bluetooth Locking Solutions. A lot can happen to a device before connections are terminated as stated by the Bluetooth Special Interest Group; The effective range between Bluetooth devices is approximately 98 feet but a more reliable operational range is approximately 16 feet [1]. From the highlighted case [2], Apple devices provide a very good estimation of the user's distance in relation to the Apple watch to trigger the unlocking mechanism without active user authentication. However, this is accomplished utilizing technologies other than Bluetooth. The utmost goal of this research will be to use only existing consumer Bluetooth hardware (e.g., Headsets, watches, fitness bands etc.), to accomplish the task of measuring and monitor the Received Signal Strength Indication (RSSI) and when the value crosses an unacceptable threshold, that is the user is now an unsafe range from their device, trigger a device lock. This is the premise of presence detection for this study. Using only existing hardware is crucial because of the now-ubiquitous nature of the technology in today's consumer electronic devices, thus the user will not have to purchase additional hardware to achieve the benefits. In this work, different techniques and applications in relation to range and the metrics that are utilized to accomplish their goals are examined. A solution is proposed, describing the methodology to accomplish the goals of this study and objectives stated above. After the proof-of-concept of the solution is highlighted. Finally the Results are presented and discussed.

2. Literature Review

In recent years, different technologies and techniques for localization and positioning have been researched and proposed. These techniques attempt to utilize attributes of the technologies such as measuring of RSSI intensity and utilizing the metric in different aspects or applying Time of Flight techniques. That is Bluetooth Low Energy augmented with the use of ultrasound to achieve their goals [3]. Bluetooth has been introduced to be a very functional and adaptable wireless protocol. To be able to utilize the wireless Bluetooth technology for

communication, a device has to be able to interpret certain Bluetooth profiles [4]. These profiles form the definitions of potential applications and govern general activities that Bluetooth capable devices use to communicate with other Bluetooth capable devices. Some uses emphasized are; wireless control of and communication between mobile devices and the class of devices referred to as headsets. This may also extend to compatible car stereos, speakers and other audio playback devices. Another foundation aspect for the development off, wireless communication with computing peripherals such as keyboards, mice and other input and output devices. Wireless control and communication among smart devices such as phone and tablets. Wireless networking between PCs and other devices in constrained environments where little bandwidth is required [4]. Some newer applications include; transmission of health and biometrics data from dedicated sensors over short ranges to phones and other capable devices. Sending advertisements from tiny Bluetooth enabled devices to other discoverable devices. Tracking using 'tags' attached to objects to determine location and personal security applications in which Bluetooth devices are in constant communication with another where broken communication results in some functionality being activated. It can be observed that Bluetooth can offer a varying degree of flexibility for different application scenarios. As such, Kurawar and his colleagues [4] resonates with the Bluetooth S. I. G [5] that Bluetooth offer a globally, interoperable solutions that address various wireless connectivity needs. Throughout this section, Different applications and techniques will be examined, the key metrics that bolsters for the attributed functionality or inhibits it.

2.1. Proximity

Proximity is always associated with some metric and a popular metric to determine proximity in relation to distance is association with wireless nodes [6]. These wireless nodes can be Bluetooth tags, Wi-Fi access points among others forms the basis to link content. The wireless nodes support standard protocols, like Bluetooth, and as such the detection of the nodes facilitates in helping to determine proximity using existing network metrics such as visibility and signal strength or Received Signal Strength Indicator (RSSI). The proximity attribute is related to its near-ness to network nodes, thus network proximity content is linked to network nodes and as such the metric of distance among nodes can be defined in this context, by its visibility in a wireless network or its signal strength. RSSI is measured in dBm and represents the amount of power detected by the receiving node [7]. Power density decreases as the distance from the transmitter increases. Thus, attempts at location estimation is done knowing the RSSI value of a node in relation to another node [7]. In comparing Bluetooth with Wi-Fi, proximity, media access control (MAC) addresses and RSSI for access points can be detected. Against proximity in relation to Bluetooth, Wi-Fi based network proximity can be utilized on a much larger range. It also proves to be quicker to detect Wi-Fi in comparison to Bluetooth. In contrast however, it lacks the capability to create Wi-Fi access points programmatically [6]. Conversely Bluetooth proximity operates on a smaller range but it allows for the creation of Bluetooth tags programmatically. For this to work on a base level, a Bluetooth device must be in 'discoverable mode'. In this mode, other devices can see device name, MAC address and RSSI. It can be observed that there was very low energy consumption as a result of a Bluetooth node existence [6]. This was attributed to the fact that energy consumption is associated with the pairing and data transfer processes of Bluetooth. Being that network proximity does not assume connectivity and subsequently data transfer, the finding regard it as an energy-safe technique. While Proximity via Bluetooth is considered more energy efficient and offers more dynamic programmability, the literature has shown it to be inconsistent. There

were noticeable RSSI degradation when moving away from Bluetooth Low Energy beacons as well as fluctuations in the environments and blockages. A noticeable point for this study was also that a fast-moving subject can miss tags which impact on the RSSI readings. As such it was suggested that Bluetooth tags should not be used for navigation related tasks. The technique is better suited for presence detection [6]. There can be many areas for network proximity deployment. One area is Ambient Intelligence (AMI), which is a multidisciplinary paradigm where different electronic objects intelligently respond to the presence of people [6]. AMI applications include the entire environment, thus accounting for all physical objects and associates it with human interaction.

2.2. Triangulation

For many applications, localization using Wi-Fi has been shown to be fairly accurate [8]. However, Wi-Fi devices are still not as cheap and widely installed on mobile devices in comparison to Bluetooth. Only Laptops and newer models of smartphones have built-in Wi-Fi capabilities while in contrast, almost every mobile phone device have an integration of Bluetooth [8]. Notably also, Wi-Fi devices consume more energy than Bluetooth devices [8], which shares similar findings with the results from other studies [6]. While Bluetooth is considered more energy conservative than its Wi-Fi counterpart, the findings from studies discussed indicate that RSSI readings may not be consistent. As such fingerprinting is advised against, for use in positioning applications [9]. Triangulation or Trilateration is a different technique attempting to provide more accurate positioning. At least three beacons and estimated distances are used to calculate the location coordinates in relation to the algorithm [8,10]. These beacons are in fixed locations throughout an area and these said beacons connect back to a centralized server, which may be referred to as the location engine. Tags are programmed to transmit a signal periodically and the frequency is determined by how real time the location estimates are intended to be. Each beacon continually reports back to the location engine all the tags it can hear, as well as the received signal strength from each. The location engine utilizes the information as well as well as the known position of each beacon to estimate the position of the reporting tags. The distances from the beacons are estimated from the signal strength are expected to map to actual distances [2].

2.3. Fingerprinting

Another area is "context-aware" computing. These contexts can be locations, identities of near-by people and objects and changes to those objects as well as information about those network nodes. This is also referred to as "Fingerprinting" [6,9] or Scene Analysis [8]. This is where signal features or fingerprints of a scene are collected and an estimation of the target location is made by matching the real-time signal features with prior collected datasets to draw results. These signal features may include the device name, MAC address and RSSI. The proximity technique discussed before, requires a large number of beacons so that the mobile device just needs to be close to at least one of them to acquire its location, as such it is considered and an expensive and difficult technique to orchestrate. As such Fingerprinting methods are more widely used [8]. In real-world applications, RSSI based location fingerprinting is used more commonly. There are two stages for fingerprinting algorithms usually. The First is scanning the vicinity or site inspection of the target environment. Reasonable points or labels are selected from the environment and appropriate coordinates and received signal strengths

(RSSI) from nearby beacons are collected. Utilizing these measurements collected from the environment, a data model is calibrated into specific features referred as fingerprints. The second stage is the run-time phase. This is where the location of a device is determined by comparing currently observed signal strengths and information from the fingerprint dataset of the first phase and the most similar fingerprint location is regarded as an estimate for the expected position [8,10]. To ensure that the technique is precise and robust, fingerprint locations should be as dense as possible. As such there exists a compromise between installation overhead against precision [10]. While fingerprinting offers to be a less expensive and the more competent technique than its counterpart proximity, there are known challenges in its utilization. The findings in the literature agree that received signal strength are vulnerable to the influences of diffraction, reflection and obstruction of the objects in the environment and even human bodies [6,8,9].

2.4. Time of Flight

Bluetooth 4.0 or Bluetooth Low Energy (BLE) has been shown to versed in communication and aid in the facilitation of many application types. Attributes such as RSSI has allowed researchers to investigate creative uses for utilizing these metrics, as was discussed. Utilizing RSSI has been shown to demonstrate deficiencies with signal propagation. Mainly issues regarding reflections, absorption and degradation of measurements accuracy with distance. On top of the RSSI metric a couple of localization techniques were developed such as Proximity and further; Triangulation and Fingerprinting. While optimizations have been made in an attempt to better the accuracy in range, there are still other techniques researched that lends to new features to the protocol. Attempts to calculate distance via the Bluetooth Protocol can not only be extracted from the RSSI but also from the 'Time of Flight' [7]. Under ideal conditions, that is line of sight and absence of reflections, RSSI samplings utilized in RSSI model-based localization techniques are testified to provide good results [7,11]. The inverse is proven though, under indoor environments, where radio propagation is said to affected by reflections on different surfaces, as such, the results of which can lead to sub-optimal distance estimation performance. As distance between devices increase, distance estimation errors increase linearly as the model has a logarithmic nature [7]. Of the techniques, a markedly different approach is to measure the distance traveled by a radio signal. That is the propagation time between the sender and the receiver. This is referred to as Time of Flight (ToF) [7]. Being that radio waves travel at a known speed, 300000 km/s, it is possible to calculate the distance traveled using the travel time, in an ideal case, this gives a 30cm degree of accuracy in a single measurement. However there exist a non-trivial area of concern. Time measurement in the nanosecond scale is considered critical with clock drifts occurring on both the sender and receiver, imposing implementation limitations [7]. To correctly measure the propagation time, a common clock reference should be used by the transmitter and receiver. If this does not occur, the trigger at the receiver side will miss the trigger to start [7]. The Techniques discussed before, aim to utilize attributes of BLE to provide some form of localization capability. However, research is being done in utilizing techniques inspired by nature and Bluetooth assisting to enhance and facilitate accuracy. Ultrasound transmissions can be considered a strong competitor for indoor positioning and tracking applications. This can have great use in sectors such as health and monitoring systems due to the accurate short-range distance measurements permitted. The 'Bat' system highlighted in [12] is based on range measurements between ultrasonic transmitters and an array of ultrasound receivers fixed at known locations and uses a multi-lateration algorithm. It computes the third dimensional positions of the ultrasonic transmitters mounted on the

user's wrists, achieving an accuracy of approximately 3cm [12]. Similarly, the 'Cricket' system makes use of beacons distributed throughout the locale while the beacons send an RF signal that assists in mapping the surrounding space all the while simultaneously sending ultrasonic signals. The receivers carried by mobile users, collect the RF and ultrasonic signals and compute their distance from the beacon using Time-of-Flight measurements. This system is claimed to be able to locate user within an area approximately one square meter with basic implementation. By increasing the beacon density, the system accuracy can be improved [12]. The 'Dolphin' system similarly consists of distributed wireless nodes that are capable of sending and receiving both RF and ultrasonic signals. It too, enable positioning of objects while achieving an accuracy of about 15cm [12]. To improve scalability and efficiency with the ultrasound techniques discussed, the positioning systems are often based on ToF measurements between a transmitter node and one or more receivers. By accounting for propagations in the range of speed of sound, time synchronizations can be done via wired connections or by utilizing wireless protocols. Due to these solutions requiring a complex time synchronization mechanism to ensure a reliable source of time, low powered wireless protocols can be considered a good candidate [12]. Bluetooth LE (Low Energy) epitomizes an effective solution for wireless implementations of the ultrasound positioning systems. This mainly due to its low power characteristics and low cost coupled with high availability in many consumer electronics [7,11,12]. During operation of the system, it performs two-dimensional positioning by using ultrasound transmission, performed by the mobile node and ToF measurements are performed by the beacons. The distance measurement procedure starts with the master node when it begins to periodically sends advertising events to the mobile node and to anchors. The observers perform a continuous scanning and process the advertising packets that are being transmitted only from the master node. Therefore, the master node can trigger the transmission and the ToF measurements [12]. Bluetooth has come a long way from its inception, has been revised multiple times and new features built upon the protocol. It has evolved from its basic use case of wireless data transfer to becoming the foundation for intelligent applications and services, ephemeral and constant. Bluetooth Low Energy marked a new era in application use for the standard. From a subset of its offerings, many applications have attempted to provide a means to locations services to fill in the gaps from other technologies such as GPS to those that can detect presence. The main facilitator for these applications is RSSI or received signal strength and from the intensity of the readings from these devices, attempts were made to deduce the position or proximity of other devices. It was noted, however, that the metric proved to be unstable and easily influenced by the current environment. Many innovations have attempted to rectify and improve on the technology to better applications. Some of these involved modifying the Bluetooth stack on one or all of the devices involved while implementing new techniques. These techniques in their own right are equally important as they have built the foundation in which new features are being added to the Bluetooth protocol stack. Other studies have claimed that RSSI is unusable for presence detection and as such should not be used. This study aims to verify these claims whether Bluetooth is feasible for presence using software and standard hardware without modification to the Bluetooth stack.

3. Methodology

3.1. Basic Requirements

It can be observed from the Literature that different arrays of solutions currently exist in different complexities and with augmentations; other hardware or otherwise, to their procedure to implement some form localization or

presence detection. These techniques range from creating customized hardware or modifying the Bluetooth protocol software or firmware stack. To get a standard functionality, the following requirements are defined; Utilizing Bluetooth RSSI readings as a metric, an attempt will be made detect the presence of a Bluetooth Low Energy device. This status of this device based on the metrics shall represent the user's proximity to the main device (referred to as the 'machine' for clarity) the software application is running on. That is, via proximity, a user's presence will be determined in relation to the machine via a range. After a certain criterion is met the application will successfully invoke the machine to lock using the machine's native lock APIs, while attempting to minimize false positives. The criteria shall be referred to the 'threshold' and the device whose RSSI metric is being tested against shall be referred to as a 'Trigger'. The application will undergo a setup procedure and after which, store the Trigger the user has opted to use. It shall also attempt to follow an automatic device choosing procedure that will choose an appropriate Trigger. After a Trigger is chosen, the application will gauge the user's presence and determine whether to lock or not. The utmost goal of this research will use only existing consumer Bluetooth hardware to accomplish the task of measuring and monitoring the Received Signal Strength Indication (RSSI) to translate to presence and when the value crosses an unacceptable threshold, trigger the machine to lock.

3.2. The Procedure

On initial start, if there is no stored information, the user will be prompted to undergo a set-up process, and store information for future use. For the set-up process, the application will utilize the Bluetooth Low Energy (BLE) radio to scan for nearby devices. If no devices were detected, an option is given to rescan or exit the application. The devices found will be referred to as Triggers. The user will be asked to select a Trigger for the run instance of the application. The Trigger will be passed to storage for future use and to the locking procedure to implement the presence detection and consequently machine locking if the need be. When a Trigger is chosen automatic or otherwise, it is passed to the locking service. This is where presence detection is done. Using attributes of the selected Trigger, a scan is done periodically to detect its presence in the environment. An interval period of two seconds was chosen as to not 'over ping' the device. From initial testing, this resulted in abnormalities and device disappearance. The Locking service implements two locking functions, both of which attempts to perform presence detection in different ways. The first, attempts to use RSSI readings from the Bluetooth scan, whereas the second attempts to perform a rudimentary technique inspired by the Fingerprinting and Time of Flight techniques highlighted by the literature. For the first locking service that performs presence detection, when the device is considered in range, nothing significant happens, however when out of range the threshold will be considered breached. This threshold value is a Trigger attribute and is calculated on first creation. It is done by subtracting a constant from the detected RSSI value during the set-up procedure. This arbitrary value will be derived from initial testing of RSSI values against distance during the testing phase of this research project. When the threshold is crossed, the machine is locked. For the second locking service, the technique will be performed in two consecutive acts. First a basic training procedure is executed to determine a nominal presence value. This is done by scanning for the chosen Trigger device every two seconds and calculating a summation of the detected RSSI value each consecutive loop. At the end of this gathering phase, an average RSSI value is determined which will then form the basis of the threshold value. This marks the end of the training procedure. The next act will utilize the threshold value produced and begin the locking service.

During this second locking service, the RSSI value will be periodically collected and averaged on every scan loop. The average is then compared to the threshold, again if this condition holds true, a machine lock will be triggered. Also, while the counterpart to this locking service utilizes a pre-calculated threshold value for subsequent run instances that will be stored, this locking method does not. As such there will be a delay before the presence detection procedure becomes active. To produce the value that will be subtracted from the RSSI values used in the presence detection techniques creating the threshold, RSSI values against distance will be compared. The normal operation positional RSSI value will be observed and the value observed at the distance beginning of the threshold range. Therefore, the threshold value is calculated as normal value subtracts distance value resulting in a difference. This difference is then subtracted from the normal value to produce the threshold value.

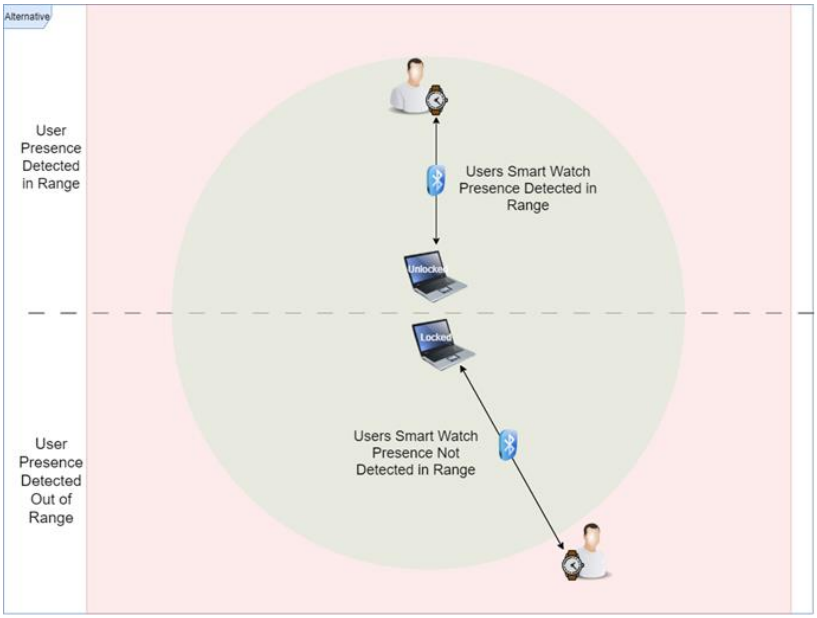

Figure 1: A Diagram showing the general states of the application.

4. Modeling

At the launch of the application there are two main cases, after which, the locking procedure occurs. This is where the presence detection is performed. At first launch, a set-up procedure is performed, during which, a threshold value is calculated for use in Locking Service 1 and the trigger is stored for future use. Subsequent launches allow for the addition of new devices or move the choosing procedure. In the choosing procedure, a Trigger device is selected and passed to either of the locking services. This may be automatic or manually chosen by the user according to the situation.

4.1. The Locking Procedure

When the user or choosing procedure has made their selection of which device to use for the monitoring, the Trigger device is passed to the locking service function. For Locking Service 1, the function is executed in a loop determining the presence of the Trigger, a Bluetooth Low Energy device. It calls the Bluetooth scanning

function and the list of devices produced is passed to the function which gets the device by MAC address, which in turn returns a list of BLE Device objects from the Bluetooth scanning function. If the Trigger device exits the threshold range, it can be assumed that the user is not a safe distance from the machine, thus a machine lock is triggered. This threshold value is calculated when the device is set-up for the first time. From the detected RSSI value, a value of eight is subtracted to be the threshold value and was calculated from initial testing. To determine the user's presence regarding a Trigger device in relation to the lockable machine, it's RSSI value is compared to the threshold value and if the threshold condition holds, it triggers a lock machine function from the which calls the native Windows lock procedure. The locking service function then pauses for two seconds and then begins the process again. If the RSSI is below the threshold, nothing gets triggered and lock service loop pauses again. For the second locking function, Locking Service 2, that also performs presence detection, a training function is called at the start of execution. Utilizing the MAC address of the selected trigger its scans to determine the presence of nearby Bluetooth Low Energy devices and get the RSSI of the selected Trigger device. The RSSI value is added to a total value and at the end of the loop, an average is calculated, determined by the number of times it was detected. The threshold value is determined from this value by subtracting four. This arbitrary value was determined by an initial testing period monitoring RSSI values in comparison to distance, similar to the other locking service counterpart. After this threshold value is calculated, the function begins its presence detection loop. It scans periodically every two seconds and every time the RSSI is detected, it is added to a total and an average is calculated. This average value is then compared to the threshold value determined from the training phase. Similarly, to its counterpart, when the average value in the threshold checking condition holds true, a machine lock is triggered, and the function pauses for two seconds. If the average is within the threshold area, nothing gets triggered and lock service loop pauses again. With regards to no device being detected, the same absent device procedure is implemented as before.

5. Results & Discussion

To reiterate, the overall operational range of Bluetooth Low Energy is approximately 16 feet [1,5]. However due to objects in an environment, the radio waves that form the basis for the Bluetooth protocol can be refracted by objects, altering the operational range of a Bluetooth device to be unique in the specific environment that the device is in. From the Methodology, two locking services are implemented, from which both, implements the capability of presence detection in different ways. For the testing phase, zones are considered. Safe zone is the normal operating position of a device and danger or unsafe zone is a range in which the machine should lock according to the presence detection algorithm.

5.1. Locking Service 1

From the experiment, using a Bluetooth Speaker as the test item, it can be noted that on a desk, in the intended natural operational placement for a specific user (the writer in this case), the speaker was approximately 10 inches or 0.83 feet (-28 RSSI) from the machine's Bluetooth radio (desktop PC with Bluetooth USB adapter located at the front of the machine). Accounting for false positives, an arbitrary distance away from the speaker marking the beginning of the danger zone was approximately -36 RSSI. Therefore, a threshold difference range of eight (8) dBm was implemented in the code. In moving away from the machine, that is picking up the speaker

and walking away from the desktop, the machine lock was Triggered at an RSSI value of -36 on average. From preliminary testing, the positional range in the environment in which the lock should be triggered, the distance of which was not measured before-hand. When the distance from the Bluetooth radio to the position in the expected lock range was measured, it approximated to 12 feet. The extremities of values, 10 inches to 12 feet occurs well within the Bluetooth's specification operational range of 16 feet. During the testing period it can be noted that RSSI values did not remain constant in the natural operational position, which agrees with the literature that there exists a jitter in Bluetooth signal and that distance range and RSSI values cannot be perfectly corelated. However, for the application use of presence detection, the device RSSI signal remained well within the expected operational boundaries. That is on the desk, the signal rarely fluctuated to a figure that crosses the threshold (the instances it did fluctuate to a value that crosses the threshold can be attributed to a false positive) and at a decent distance away from the machine, a position expected to be the lock range, fifteen feet away, the measured RSSI value would cross the threshold within a few inches.

5.2. Locking Service 2

Like locking service 1, the test device and locking zone are also the same for this testing phase. A key difference is the threshold parameters implemented in the algorithm. In the normal operational placement, the speaker is still placed 10 inches away from the BLE radio. However, it was observed there were almost no false positives. As such it can be attributed that this technique of averaging RSSI values stabilizes the jitter of values detected. This can allow for a shorter range from the normal operational position to enter unsafe zone as such the differential range value from normal was calculated to be four (4) dBm from the normal operational RSSI. From the training procedure at the start of the locking service, the normal operational RSSI figure was detected to be -28 and accounting for the allowance of a shorter range to enter the danger zone, a threshold value was calculated to be -32. In moving the test device away from normal position, it was observed, as expected on entering the threshold range, the machine was locked. The distance when measures was at approximately 5.5 feet.

5.3. Comparison and Contrast

For both presence detection techniques implemented via their respective locking service, it was observed that when the threshold value was approached, that is the test device entered the unsafe zone, the machine would lock with no significant delay. This is expected as at the end of presence detection loop the determining factor comes down to the comparison of two values. However, a noticeable difference is the range required to operate correctly. Measuring the fluctuations of the RSSI values in the normal operating position, it stands to reason that if a false positive detection occurs, that is the device is not moved, the machine would be locked. That would be considered annoying to the user and diminish use case functionality. Thus, during observation, utilizing the lowest range difference values from false positives was factored in creating the subtraction range for the first locking function. The second locking function does not suffer from the RSSI fluctuations, as such a tighter useable range could be afforded for this function. The training value would represent normal use case position and a differential range value of four would account for a small degree of movement by the user in proximity of the device but still be registered as present by the algorithm. However, an average value when calculated would

cross the threshold soon after the user has left the safe zone, thus indicating their presence is no longer near the scanning machine.

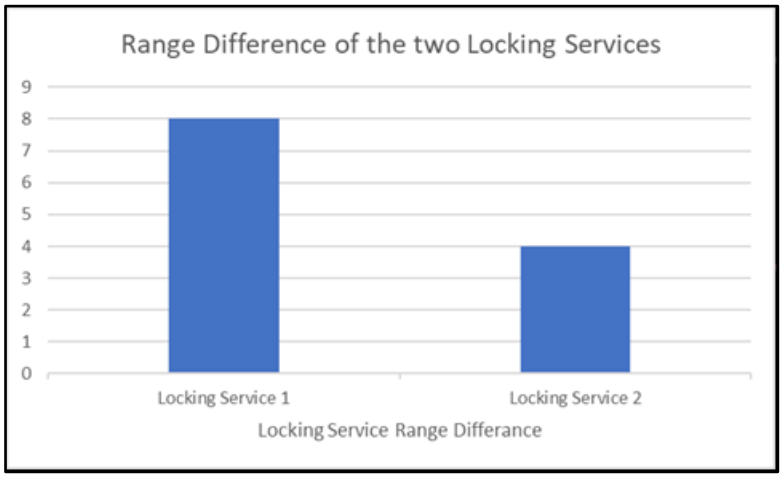

Figure 2: Showing the Range Differences of the two implemented functions.

A major difference between the two techniques is their registration to user's return to the safe zone. For the first locking service it is almost instant when it detects the device and notes the device's RSSI is not at a range that should trigger the machine lock, thus not holding the machine lock, allowing the user to sign into their machine. Inversely for the second locking function, the behavior of its counterpart does not occur. When the device returns to the safe zone the machine lock is still held for a period of time. In testing, for a device moved out of the safe zone for 2 seconds and then returns to the safe zone immediately after, the second locking service maintains the lock of the machine well over two minutes, 120 seconds, thus preventing the user to sign into the device. This can be attributed that the average would become 'stable' constant, as time passes, thus the decision was made to clear the values every 30 seconds so that changes can be recognized more quickly.

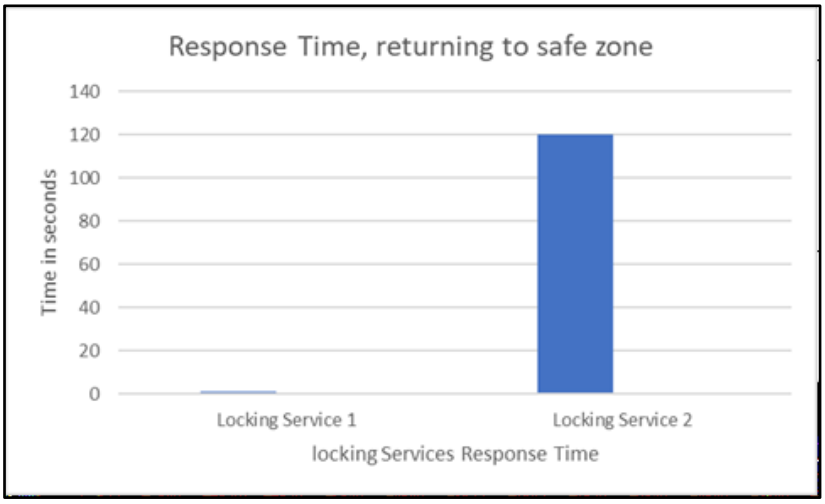

Figure 3: Showing the Response Time Differences of the two implemented functions.

6. Conclusion

As different classes of devices are used to do work and play, the generation of sensitive information and media does not halt, as such different technologies and techniques are used to protect those devices. Such protection mechanisms however have different compromises to convenience as is often the case with increasing security. Utilizing existing, ubiquitous consumer Bluetooth hardware to complement these security measures can offer a degree of flexibility and convenience to these existing authentication techniques by offering the capability of presence detection of a user without the use of additional and customized hardware, which can drive device prices up and fragment security features to premium products only. In this thesis, a Bluetooth Low Energy (BLE) locking method has been implemented while performing presence detection has been proposed and described. According to the literature, useful ranges of Bluetooth devices can vary significantly with environment and conditions for use. While BLE is focused on short range communication, as such an estimated typical operating range is approximately sixteen feet, the experiment of this work does indeed agree with specifications, as there is not a need for long distances to determine device presence to initiate a machine lock well within the parameters. This can actually be considered beneficial and good for the use case providing Bluetooth firmware behaves consistent across devices. This work contrasts with similar themes and improves on existing functionality that depend on the complete loss of device connectivity to determine the lack of the user's presence even without a connection to a device. This study also builds on idea that presence detection using the Bluetooth Low Energy is feasible even once the application parameters are understood and highlights that accuracy of future application will increase. While this work mainly focused on the use of BLE devices for user presence detection, there are many justified cased for this use and capability. Among them may include the ability to detect devices in a fleet. This has heavy implication in the realm of internet of Things (IOT). Researchers can place sensor devices that may utilize Bluetooth Low Energy and have another device periodically detect them to ensure the cluster is operational and present. The system can even go further to have a near real time system to alert the user that there is a problem in the cluster. This is can be considered similar to 'heat beat' functionality used in the server space. The use for near presence detection capabilities can be widely creative and functional.

6.1. Future Work

While this work focused on Bluetooth Low Energy 4.0, this can be considered antiquated in the computing and technology field. Bluetooth 5.0 has been released in 2016 with version 5.1 in 2019 [5]. However, devices and radio adapters utilizing this new specification is not yet widely available. As such work incorporating the new features such as Angle of Arrival (AoA) and Angle of Departure (AoD) can help to increase accuracy [5]. User presence applications can also tap into the IoT field to have more integrated and autonomous actions being executed for the user.

References

[1]. K. Townsend, C. Cufí, and R. Davidson, Getting started with Bluetooth low energy: tools and techniques for lowpower networking. " O'Reilly Media, Inc.," 2014.

[2]. T. Hollingsworth, “Apple Watch Unlock, 802.11ac, and Time,” The Networking Nerd, Sep. 21, 2016. https://networkingnerd.net/2016/09/21/apple-watch-unlock-802-11ac-and-time/ (accessed Dec. 07, 2020).

[3]. A. Comuniello, De Angelis, Alessio, De Angelis, Guido, and A. Moschitta, “Ultrasound Time of Flight based positioning using the Bluetooth Low Energy protocol,” in 2019 IEEE International Symposium on Measurements & Networking (M&N), 2019, pp. 1–6.

[4]. A. Kurawar, A. Koul, and V. T. Patil, “Survey of bluetooth and applications,” Int. Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 3, no. 8, pp. 2832–2837, 2014.

[5]. S. Bluetooth, “Enhancing Bluetooth Location Services with Direction Finding,” Bluetooth Special Interest Group, Tech. Rep, vol. 1, 2019.

[6]. D. Namiot and M. SnepsSneppe, “On Bluetooth proximity models,” in 2016 Advances in Wireless and Optical Communications (RTUWO), 2016, pp. 80–84.

[7]. D. Giovanelli and E. Farella, “Rssi or timeofflight for bluetooth low energy based localization? an experimental evaluation,” in 2018 11th IFIP Wireless and Mobile Networking Conference (WMNC), 2018, pp. 1–8.

[8]. L. Zhang, X. Liu, J. Song, C. Gurrin, and Z. Zhu, “A comprehensive study of bluetooth fingerprintingbased algorithms for localization,” in 2013 27th International Conference on Advanced Information Networking and Applications Workshops, 2013, pp. 300–305.

[9]. Iglesias, Héctor José Pérez, V. Barral, and C. J. Escudero, “Indoor person localization system through RSSI Bluetooth fingerprinting,” in 2012 19th International Conference on Systems, Signals and Image Processing (IWSSIP), 2012, pp. 40–43.

[10]. D. F. Serhan and A. T. Cemgil, “Modelbased localization and tracking using bluetooth lowenergy beacons,” Sensors, vol. 17, no. 11, p. 2484, 2017.

[11]. D. Giovanelli, E. Farella, D. Fontanelli, and D. Macii, “Bluetoothbased indoor positioning through ToF and RSSI data fusion,” in 2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN), 2018, pp. 1–8.

[12]. A. Comuniello, De Angelis, Alessio, De Angelis, Guido, and A. Moschitta, “Ultrasound Time of Flight based positioning using the Bluetooth Low Energy protocol,” in 2019 IEEE International Symposium on Measurements & Networking (M&N), 2019, pp. 1–6.