Annals of Emerging Technologies in Computing (AETiC)
Vol. 2, No. 2, 2018

Long Article

Intra-building People Localisation Using Personal Bluetooth Low Energy (BLE) Devices

Glebs Kuzmičs[1] and Maaruf Ali[1, *]

[1]Faculty of Architecture, Computing & Humanities, Univ. of Greenwich, London, SE10 9LS, UK
glebskuzmics@gmail.com
[2]Dept. of Science & Technology, Univ. of Suffolk, Neptune Quay, Ipswich, Suffolk, IP4 1QJ, UK
*Correspondence: maaruf@ieee.org

Received: 27th February, 2018; Accepted: 9th March, 2018; Published: 1st April, 2018

Abstract: This paper discusses the conceptual implementation of a system to locate people inside buildings using their personal Bluetooth® low energy device(s) in situations of a crisis. Various aspects of BLE technology are covered with regard to their usage for emergency management. Legal, social, ethical and professional issues are also discussed in using this technology, especially in matters of safeguarding information privacy. The plan of the proposed system is then discussed and concluded.

Keywords:* *Localization; Bluetooth Low Energy; BLE; Location Based Services; LBS; Crisis Intervention

1. Introduction

This project aims to enable the use of Bluetooth® Low Energy (BLE) enabled device(s) to locate people indoors during and when recovering from an emergency. The constant availability of BLE in wearable and mobile devices allows for procedures whereby it is possible to aid the emergency services to locate and identify the victim or person in need of assistance.

The window of opportunity can often be too short to locate, tender medical aid and rescue the person. The project enables better use of this time by leveraging hardware and software based solutions for tracking people indoors using BLE frames from users' devices. There is a high probability that a functioning device will still be in the users' possession - thereby helping to get to them quicker.

The lives of people are at risk due to a variety of emergency crises, for instance, evacuation procedures, earthquakes, collapses of buildings, fires, explosions, terrorist activities, etc. Every minute matters, there may not be a lot of them. The proposed solution applies diverse methods to significantly improve the situation of locating a person in a short period of time.

The proposed system utilizes a wireless 802.11s mesh of Raspberry Pis to capture Eddystone BLE frames, these are continually broadcast from the users' devices. Thereby the location can be deduced by environmental variables. The application of BLE for the purposes of people localisation indoors is not innovation, but this project is an attempt to avoid the pitfalls with indoor localisation and navigation techniques that currently utilise BLE technology. For this reason, the project

Glebs Kuzmics and Maaruf Ali, "Intra-building People Localisation Using Personal Bluetooth Low Energy (BLE) Devices", Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 24-36, Vol. 2, No. 2, 1st April 2018, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2018.02.003, Available: http://aetic.theiaer.org/archive/v2/v2n2/p3.html.

proposes the adoption of the following two approaches; the use of the RSSI (received signal strength indicator) fingerprinting and proximity determination.

The primary aim of this project is to develop an understanding of BLE with a focus on locating individuals during an emergency. Furthermore this project is restricted to open source hardware and software. The open source software allows the proposed system to be both transparent and to be available for everyone for further development and contribution and also to meet a greater diversity of uses for the future of the project [1].

2. Overview of BLE (Bluetooth Low Energy) Technology

BLE technology can be summarised as:

- A wireless computer networking technology;
- A component of the overall Bluetooth Smart stack, along with the classic Bluetooth and high-speed Bluetooth protocols [2].

Devices are divided into two groups; Bluetooth Smart Ready and Bluetooth Smart. Bluetooth Smart Ready in most cases indicates dual-mode devices (usually laptops, tablets or smartphones), which have hardware compatibility with classic and low energy Bluetooth peripheral devices. Bluetooth Smart generally indicates only low energy devices, for instance a temperature sensor, which requires a central or peripheral device for functioning [2].

From a physical point of view, BLE and classic Bluetooth are similar. The radio frequency band used is the ISM (industrial, scientific and medical) 2.4 GHz, which allows for a single antenna to be used. Their difference, however, lies in how the frequency range is subdivided: BLE uses 40 channels of 2 MHz bandwidth, on the other hand classic Bluetooth uses 79 channels of 1 MHz bandwidth each. The differences also extend to the modulations used. This results in BLE and classic Bluetooth being incompatible with each other. The modulation and wider bandwidth of the channels allow BLE to operate at a lower maximum power level of 10 mW, whilst still having a throughput of 1 Mbit/s [3]. From a networking aspect, BLE is a stateless protocol. This allows for data sources to operate on a fire and forget principal. This permits flexibility for the topology of scanners increasing flexibility. Another advantageous aspect of BLE is flexibility in terms of support among various devices and platforms. BLE can be integrated into existing products and extend its functionalities [4].

Corresponding to its name, BLE technology provides lower energy consumption that allows devices to be autonomous and functional for a long period of time. For instance a BLE beacon can operate for up to two years using a coin cell battery. However, the energy consumption depends on the settings that are used when and the frequency a device transmits data, or as in the case of beacons – advertises data by transmitting advertisement packets to nearby listening devices, more frequently or at a higher power, it consequently uses more energy and vice-versa [5].

The use of BLE are divided into four rôles [6]: viz.: Broadcaster, Observer, Peripheral and Central Device. Peripheral and Central devices are important for this project.

Peripheral – these are devices that are usually placed at the outside layers of the topology. These devices mainly perform the following actions: advertising to neighbouring devices that they contain some useful information and are waiting to be connected. Peripheral devices have to be optimized in terms of energy consumption in order to stay autonomous for a long period of time. As an example, a temperature sensor that is located in a public place advertises that it contains data. A person can subsequently scan for devices using smart devices (for instance a smartphone), then connect to the peripheral device and download the data from it (in this particular case the actual temperature values) [6].

Central: these devices take a master rôle in the topology and as its name suggests, are located in the middle hierarchically (usually logically) and surrounded by peripheral devices. These peripheral devices wait for connections from the central device. A central device may be considered as one complex device that can run multiple connections [6].

In order for the correct routing of information between the devices, addressing is important and mainly is used for identifying an advertiser. Each BLE device has an address assigned to it; the identification process is straightforward. Addresses can be separated into two groups: random and public. Random addresses can be further divided into private and static. The same format in MAC addressing of having 48-bit addresses are used in BLE technology [7].

BLE beacons are found useful in airports and stations, where they are utilized to identify passengers. Especially in order to help them not to miss their flights while being stuck in the security queue, as well as to avoid missing connecting flights for transit passengers in case the boarding gates have been changed unexpectedly. An ancillary benefit to having beacons deployed is using their UUIDs (universally unique identifier) to correspond to audio guides for individuals, who require such additional help [8].

2.1 Structure of BLE Frames

Fig. 1, below, shows the structural breakdown of the various fields that make up a BLE frame. The main ones are described below:

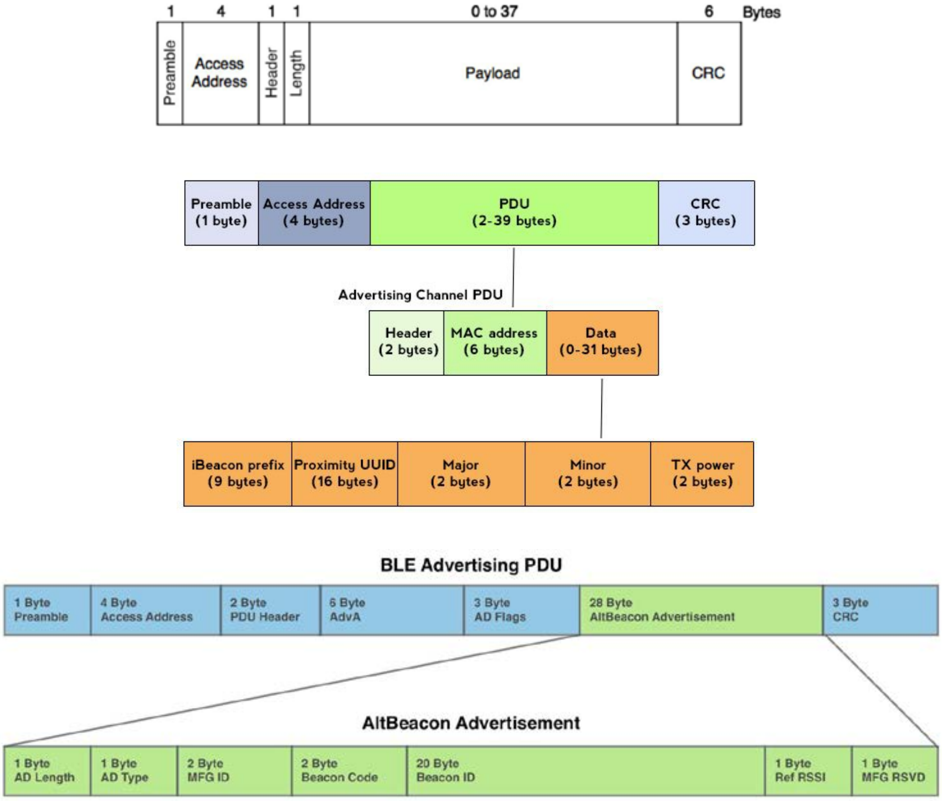

Figure 1. The Fields of the BLE Frames.

- Preamble – this is a specific training sequence that indicates the start of a frame.
- Access Address – this is utilized for distinguishing the frame from background noise, as well for identifying the type of the frame – for example an advertisement frame.
- Header – this is utilized for indicating the type of the frame.
- Length – contains the length of the following frame.
- Payload –the actual information contained or carried in the specific frame.
- CRC (Cyclic Redundancy Check) – utilized for ensuring that the payload of the transmitted frame does not contain errors or has not been changed during the transmission process [9].
- There are several implementations of BLE beacons, for instance: iBeacon, EddyStone, AltBeacon and URIBeacon. These implementations vary not only by standards used, but also by cost (some of them are free, some – proprietary) and there are related advantages and disadvantages associated with each type of BLE beacon [9].
- Proximity UUID – identifier that is used to distinguishing one company's beacons from others, for example, the beacons in a chain of stores will all have the same proximity UUID.

- Major – used to group beacons; for example, beacons located in stores of the shopping mall can be put in a group, which allows a mobile to identify in which specific store the customer is actually in.
- Minor – used to identify the individual beacons; that allow to localise a customer in that specific store.
- TX power – used to identify how close the central device (in this case, the customer's mobile device is to the peripheral device (BLE beacon). The TX power is measured as the strength of the signal at a distance of 1 m from the device [9].

Eddystone is an open-source protocol, its source code and specification can be accessed at github.com/google/eddystone [10].

There are three types of frames in the Eddystone protocol which significantly differ from iBeacon advertisement packets; Eddystone supports multiple frame types: Eddystone-URL, Eddystone-UID and Eddystone-TLM. There is also a secured version of the Eddystone-UID, the "ephemeral" (Eddystone-EID) [10]. The pertinent properties of the Eddystone frame are:

- Unlike iBeacon, which officially is only supported by iOS, Eddystone provides support for both platforms (Android and iOS).
- Eddystone-UID is targeted towards providing an identifier that may be used as a trigger for an application on mobile devices It consists of two parts: namespace (10 bytes) and instance (6 bytes) which results in a total size of 16 bytes and unlike, iBeacon's 20 bytes advertisement packet, which contains three components.
- Eddystone-URL is used to advertise URLs. It consists of one field of variable length in order to accommodate various URL lengths. Unlike iBeacon and Eddystone-UID, Eddystone-URL does not require an application to translate the beacon's identifier for actions to be triggered.
- Eddystone-TLM is transmitted with the Eddystone-UID or/and URL frames and is utilized for informing that device management is required. This is implemented by broadcasting the telemetry values that include: the battery voltage, beacon temperature, uptime and number of frames sent since last power-up or reboot.

For deployments requiring additional security Eddystone-EID can be used. It shares a ephemeral identifier, which must be responded to by the correct API key using Diffie–Hellman in order for the beacon to transfer the data it contains. In case of iBeacon no specific features for security measures are utilised; frames are transmitted using public signal and can be easily accessed from iOS and some Android devices [10].

2.2 Approaches taken by BLE

Solutions that use fingerprinting are considered to be the most accurate in terms of lower index of distance errors. Positioning systems that are based on fingerprinting can be divided into two phases: off-line and on-line. During the off-line phase, the location is fingerprinted and the collected data is divided into rectangular grids. As well as the RSSI is collected at each of the grids by Multiple Access points. The second phase, on-line, is responsible for the comparison of the actual RSSI value that is received by a user's mobile device at the present position and the results that were collected during the off-line phase. Next, the application examines the values, which are stored in a look-up table and finds the nearest surrounding point that returns the present location of the user [11].

The approach, which is utilized for indoor localization is called the radio propagation model based method; a simple mathematical expression is applied which represents the relationship between the RSSI and the distance. However, some limitations exist, especially, when the RSSI is affected by various environmental conditions, as a result, the precision is affected [12].

The second approach that is utilized in BLE technology is trilateration, however, this is not that widely utilised as fingerprinting and mostly used in GPS navigation systems. This trigonometric approach applies triangulation for tracking objects. The accuracy directly depends on the environment conditions and the quality of the received signal [12].

But what is the difference between the RX and RSSI values? Both are used to measure the strength of the radio signal, both of them indicate the power level, which is received by the antenna. However, RX is measured in mW (milliwatts) or dBmW (decibel-milliwatts), but the RSSI is a percentage of the signal strength. So the higher the RSSI value is – the stronger the signal. In comparison to RX, RSSI is just a qualitative measurement, which in most cases is defined by the manufacturers and there is no intrinsic physical parameter for this value. For instance, a device may provide a range between X and Y, as defined by the manufacturer. The range of value can be mapped to a percentile range describing the signal quality from the view of the device RSSI and this can be mapped to particular and physical RX value, which would off course vary by device due to their physical differences [13].

3. Literature Review

Filippoupolitis *et al.* [14] proposes and practically proves the approach that people localisation indoors is possible without the need of using any standard localisation processes in mobile phones. Instead of it, the data is sent to a remote server, where it is processed using calculations of the building occupancy using the classifier that has been initially trained during the data gathering phase. The results of practical experiment show that utilising machine learning techniques in combination with BLE technology has a promising potential for accurate indoor localisation. Also the potential of this approach indicates that utilisation of it can contribute to changing emergency management to be more efficient, excluding one of the potentially vulnerable technique, which can fail in case of emergency, leading to the overall reliability and stability of the system [14].

The project by Lin *et al.* [15] utilised a standard set of hardware: BLE beacons, staff and patient mobile devices, remote system server and mobile application of two types (member of staff and for patients). The product that had been developed is a mobile-based indoor localisation system, which allows to track patients utilizing mobile application that is a iBeacon-based solution. Mathematical algorithm that has been used in this project allows the localisation system to function with an accuracy of 97.22% (location classification). Predicted errors between subareas of the environment used during the practical experiment do not exceed 5 m; in real world scenarios these numbers can vary, depending on the complexity of the building [15]. The project is based on the RSS method because of its relative simplicity and accuracy in comparison to other methods of localization. The values of the RSSI are obtained from the beacons and location is then estimated. The iBeacon selection stage, which is deployed on RSSI values, can be divided into three steps: signals collection, selection of the nearest beacon using mathematical algorithms and uploading the values from the estimated nearest beacon to the system server, where the data will be processed and the nearest beacon estimated using a beacon-location mapping table [15].

The above project has a potential because of the way of deploying the localisation system using the basic set of components, which are understandable in implementation and configuration, as well are cost effective. By applying the mathematical algorithm, the authors have achieved high accuracy of the system, which is essential in the case of hospitals, especially, emergency rooms, allowing members of medical staff to track and locate patients efficiently.

Critically evaluating this project, the benefits appear to prevail the disadvantages. The project's simplicity in terms of components and their deployment, as well as exhibiting a significantly low level of errors in accuracy allows this project to be considered as a finished product for utilisation in hospitals. Also there is a potential for application in a wider scope of businesses. The localisation system can be used in various combinations, for instance, BLE or Wi-Fi only, as well as using the data combined from both technologies [16].

In comparison to other projects, which utilise Wi-Fi and fingerprinting of an environment, the proposed solution shows better results and demonstrates that information combined from two systems allows to have an almost excellent level of localization accuracy [16].

To make the working process more efficient HTML5 and CSS3 based front-end application was developed. Furthermore in order to provide stable handling of the localisation engine and managing the service of a smart library, a back-end server application has been utilised. As a server-side framework solution the authors have adopted Node-RED from IBM. According to the authors, the main reason for choosing this application is its functionality and flexibility [16].

In order to show the perspective of using the combination of technologies in detail, the review of Kriz *et al.* [17], proposes that use of different types of radio based indoor technologies provides an improvement of accuracy over the use of existing Wi-Fi systems by adding BLE beacons. The proposed method shows not only the improvement of the accuracy, but also it decreases the overall number of areas, which are not functional for localisation due to the inability of Wi-Fi signal to propagate within complex environments. The results of the practical experiment show that the combination of BLE and existing Wi-Fi setup for localisation purposes improves the median accuracy by 23% and reduction of a variance [17].

By combining two technologies the project cost can be more efficient, as applying BLE beacon with existing Wi-Fi infrastructure is more cost saving then making significant changes to it. Also the method has a great potential of adopting the system to larger environments: shopping malls, factories, offices and construction sites - in order to minimize the distance range limitation of BLE by combining it with Wi-Fi. The proposed project can be well applied for the purposes of emergency management as increase of the overall accuracy is essential [17].

In the following paragraphs the utilisation of BLE technology for the purposes of Wireless Body Area Networks (WBAN) aiming at safety of emergency units will be discussed. The work of Rius *et al.* [18] mainly scopes towards modifying the original design of antenna that is used for WBAN in order to increase the initial frequency and create smaller, more flexible and comfortable solution. The provided examples are aimed at integrating sensors and network nodes into clothes of members of staff of an emergency unit, for instance, clothes of a firefighter, where sensors are interconnected with a smart device (in the case of the research – a watch) via BLE. The system can monitor thermal stress level, exceeding of which will cause the alarm triggering and user being notified [18]. The authors provided information about four practical experiments: body issues, flexibility, textile and thermal stress tests. This type of system can be utilized in extreme conditions and has to be reliable, as in some cases emergency team members' lives may depend on it [18].

The research of Chandel *et al.* [12] is scoped towards calculating the shortest path indoors based on a machine learning method that is utilised for estimating the distance from BLE beacons. The solution is generally aimed at being integrated into systems, which allow customers to find their path indoors, as well as to track position in real-time mode. The solution can be perfectly adopted with a meeting planner. The system can be configured to one of the possible ways of utilisation is emergency management, for instance, the system can be applied for routing, tracking and guiding in case of evacuation [12]. The proposed system is RSSI measurement based but unlike other solutions, RSSI measurements from BLE beacons are used in combination with public sensors. This approach allows the system to have a minimised level of localisation error [12]. Vector models converted from a rasterised form are used as building floor maps. This allows avoiding the need of developing complicated techniques. This feature is advantageous, as it makes the system more efficient in terms of developing and scalability for larger environments, which also require a larger indoor map. In most projects, conversion is done manually that in case of large buildings and larger floor planning increase the possibility of errors. In order to avoid it, the project's authors have implemented the algorithm that is used to vectorise the floor maps. Special filter for dividing the areas into walkable and non-walkable (valid and invalid) parts is utilized [12].

Not to have a direct relation to emergency events, all of them can be applied to the solutions that will contribute to the working process of emergency services and increase efficiency of rescue operations, evacuation procedures and tracking people indoors in case of activities that can cause victims, e.g., armed assaults, robberies, terrorist attacks.

4.1 Legal, Social, Ethical and Professional Implications of the BLE Localisation System

All legal, social, ethical and professional aspects are pretty abstract, as preservation of people lives takes priority over them in an emergency. However, assuming that legal, social, ethical and professional issues can be ignored in case of emergency events and when persons' lives are in risk, ignores the system's normal mode of operation, as the operation of the system is planned to be persistent, non-EMS use of the system may be impacted by legal, social, ethical and professional issues. The most important and affecting issues are the legal aspects, as the proposed system may involve persons' data. The data gathering process is affected by the Data Protection Act. However, as it is planned at the practical implementation stage, the data that will be transmitted from the persons' mobile devices which will contain links to their public pages, for instance, social networks. This means that this type of data is publicly available. This method will aid emergency services to identify people, who are in risk due to the emergency event; also, using information from a public page, next of kins' contact details can be found for example through Google Person Finder.

Taking into consideration the fact that the type of data transmitted from mobile devices and gathered by emergency services might be changed and may need to contain personal data of persons, a high level of data protection is required to be implemented. For this purpose opportunistic encryption will be used.

4.2 Analysis of the BLE Localisation System

The first approach is based on the RSSI fingerprinting method. It uses a similar method that is utilised in indoor localization and navigation system based on BLE beacons. But in terms of the project user's mobile device which acts as a beacon all the proposed solution will operate in the opposite way, wherein the mobile device will act as a portable BLE beacons and the Raspberry PI will operate as the receiver of the signal. This approach can be divided even further, namely, two fingerprinting methods: the first method can be considered as less precise in terms of localisation, as RSSI values will be gathered for a single room as one entity. This method requires less implementation effort and time spent. The second method is based on the same fingerprinting technique, but involves dividing a room into sectors. So a person's location can be determined more precisely, not just tracking in which room a person is located. Of course, the second method requires assigning RSSI values to multiple sectors in each of the rooms; also more system and network performance is needed for this method - as more data has to be stored, processed and transmitted.

The choice of the method mostly depends on requirements of the project, as well as on size and complexity of environments, where the system needs to be installed. For instance, the first method can be implemented in office buildings, hotels, etc., which usually have small size, standard rooms, where less precise localization techniques can be considered. The implementation of the second method is more suitable for projects with larger environments, for example, shopping malls, stations, airports, hospitals, as application of the first method will not be rational and its general approach of tracking people is not suitable due to the size of the environments and lack of precision. One of the benefits of utilizing this approach is in utilisation of Raspberry Pis as a part of the system. First of all, it allows to move away from the need of using proprietary solutions and allows the system to be not only open-source based, but become more flexible and easier to adapt to the needs of the project and the user(s). In some case a remote server with a CMS (content management system) is involved in a process, but usually interconnection between mobile devices and a remote server is done utilizing a Wi-Fi network. But this can become non-functional due to power outage during an emergency; so in both cases localisation method that utilizes BLE beacons is not helpful for crisis intervention.

In case of utilising the first approach proposed by the author, localisation data can be accessed by emergency services, as the data is transmitted via network cables or wireless network (or both for higher level of redundancy). If both network options fail, there is a possibility to directly connect to Raspberry Pis and access the localisation data. In the worst-case scenario, when all BLE receivers (Raspberry Pis) are damaged and non-functional, the second approach becomes the main method for people localization.

The second approach is fully based on proximity determination and can be utilized between two mobile devices – one-to-one option, when a member of emergency services is tracking for one person, or many-to-one, in case when several members of a rescue team are tracking the location of one person. The principle of the process is pretty simple – the person's mobile device is acting as a

BLE beacon and transmits the signal, the rescue team member's device operate as a receiver showing the nearby devices, which have Bluetooth modules enabled and are also transmitting BLE signals.

Raspberry Pis will be utilised to develop a localisation system for tracking people indoors. The main rôle of these devices is in operating as receivers of BLE signals, as well as processing of the collected data and transmitting it to a remote server that is utilized by emergency services. Raspberry Pi 3 Model B has been chosen as an option for a receiving device; as it has built-in Wi-Fi and Bluetooth 4.1 modules. Its benefits are obvious: these modules are essential in terms of this project to the requirements of utilising BLE interconnections as well as creating wireless networks between Raspberry Pis.

Regarding the topology for interconnecting Raspberry Pis that are operating as receiving devices, there are two options that may be considered. First, the simplest option in terms of installation and configuration at the client site (environment, where system is installed and ready to be used by emergency services in case of some event); each Raspberry Pi is installed in a room and receives the BLE transmitted signals from mobile devices, all the data collected is transmitted to a remote server, where it is processed and can be used in case of emergency. Mobile devices (smartphones) based on the Android operating system will be used as transmitters for both approaches. In terms of the second approach, mobile devices are utilised as both sides of the BLE process, as transmitting and receiving. The number of devices to be used during the experiment will be determined in the course of practical stage, but in terms of the real life project, the number of devices directly depends on the size of an environment and the number of users located inside an environment. Also it might be useful to implement a list of UUIDs of devices that are installed in the environment and Bluetooth modules transmitting. This will contribute in avoiding a situation when the emergency services follow the wrong localisation data and the person in trouble can end up receiving delayed aid.

The following assumptions are made for the successful implementation and operation of the BLE locating system, that:

- The mobile application, which is utilized to transmit the BLE signal is installed on every person's mobile device, is always active and transmits a signal.
- In case of the transmitting BLE signal, which might contain private data (name, surname, contact, medical details), the person agrees that in case of an emergency event the information from a mobile device will be shared with the emergency services.
- If a mobile device is functioning (in terms of the project – BLE signal), or is damaged, but still functioning, the owner is alive, but is immobilised by various factors (parts of collapsed building, hostage taking, etc.).
- All the collected data about people location indoor is transmitted to a remote server, which can be accessed by emergency services; during rescue operations, evacuation, etc. This can contribute to the efficiency of finding people inside a building by using their current or last known locations.
- Stationary mounted Raspberry Pis are placed in shockproof cases to minimize the risk of damage and becoming non-functional due to the environment collapse or similar causes of emergency events.
- Each Raspberry PI is equipped with a battery, it is considered that the risk of the system's unavailability due to the power outage is avoided; by doing this, the redundancy of the system is improved.

Regarding the first approach, the Raspberry Pis are stationery and located in each of the rooms where they perform the BLE signals' receiving function. The users' mobile devices act as the BLE beacon by transmitting BLE signals. This approach can be applied at the early and ongoing emergency events, namely, until the structure of the building is not changed due to the variety of factors (explosion, earthquake, collapse, etc.). In most cases while Raspberry PIs are not completely damaged and are still functioning and receiving BLE signals from the users' mobile devices and transmitting data to a remote server (or at least storing it), this approach can then be considered as working and rational. The examples of the real life situations are the followings – evacuation procedures due to the risk of a potential emergency event or at in their early stages; when the emergency risk is escalating and cause casualties among people located inside the building; in this type of situations the first approach will contribute to emergency services in tracking, finding people indoors and evacuating them as quickly as possible.

The first approach can be utilized at the later stages of an emergency event as well, but many factors can cause shortcomings in the system's functioning, for instance, power outage can cause network components shutdown. If there are no redundancy actions taken, the emergency services will still be able to access the Raspberry Pis directly, locate and rescue them.

The second approach, in which the proximity determination technique is utilised, can be considered as an alternative option. It can contribute to the success of a rescue operation in case of the building's change of the structure due to the factors that have caused serious damage. The possibility that people are trapped under the layer of building material is very high, so the rescue teams need a way to know how to track people before starting their rescue procedures. These have to be performed with a high level of accuracy, as mistakes can cause more collapses and thereafter more casualties. Surely, proximity determination technique cannot provide a method with excellent accuracy, but it can help minimize the area of search, thereby the rescue procedures can be started quickly and the trapped people will be rescued sooner hopefully.

5. System Description

The setup proposed for the experiment consists of four Raspberry Pis (three of which are used for receiving BLE signals from mobile devices and one operates as the central device that receives data, processes it and transmits it to a remote server utilised by the emergency services. The next components that can be seen are mobile devices with installed mobile application that enables the beacon function and transmits BLE signals.

Interconnection between devices is done utilising wireless technologies – Raspberry Pis are interconnecting by Wi-Fi (network cable interconnecting is considered for better redundancy). BLE technology is utilised between transmitting mobile devices and receiving Raspberry Pis. This topology cannot be considered as point-to-point connection, as the mobile device operate as BLE beacons and each of the surrounding devices can receive a signal. However, by utilising fingerprinting method and assigning RSSI values to each of the rooms, this can help to solve this issue. In other words, each receiving Raspberry Pi will be able to distinguish RSSI values assigned to the room, where it is located, from the neighbouring rooms.

The second scheme consists of the mobile device of a user (the potentially threatened person) operating as a BLE beacon and transmitting a signal, meanwhile the emergency team member's mobile device's main function, during a rescue operation, is in receiving the signal. Using proximity determination by RSSI values and applying calculations - the approximate distance to a person can be determined. Also multiple devices can be used on both sides. As BLE is a wireless technology, in which signals are multicast from one device to the surrounding devices, the principle of operation does not differ between the device-to-device method and utilization of multiple device method. Utilizing the proximity determination approach can be helpful in reducing the area of a rescue operation, thus time that needs to be spent and success of the operation can be improved. But in real-life conditions many factor will be affecting the accuracy. For instance, in the case of building collapse due to an earthquake, the propagation of the BLE signal will vary because of the thickness of the building materials and walls.

The mesh network of the proposed system also utilises an internal backend server network using IPv6 networks that are also interlinked by the IPv6 Internet. The attributes of IPv6 that impact these networks are the extended address space and the Neighbour Discovery Protocol (NDP). The extended addressing provides additional flexibility without the need of the burden of using NAT (network address translation) configuration, which results in a faster network convergence. NDP allows for the operation of a 'no acknowledgement' network, which improves security. Additionally using global IPv6 addresses simplify the identification of a devices network location, which would allow for a flexible data collection in the event that the emergency was to be catastrophic. During a condition of anomaly, for example, system destruction occurs, EMS (emergency medical services) personnel will be able to connect directly to Raspberry Pis due to the use of global addressing.

The process of transmitting the BLE data collected from devices of users from scanning Raspberry Pis to the backend server can be divided and described using the following four steps:

i. BLE script that is implemented on each of the scanning Raspberry Pis dumps the raw data collected in to the local Interplanetary File System (IPFS) nodes pubsub. IPFS is cryptographically linked, that means it is immutable and permanent.

ii. The raw data is made available over the mesh network.

iii. The raw data is taken in by a pnode and it is decrypted and verified and then it is offered up to BigchainDB.

iv. Because it would be insecure to have a pnode that is public facing, due to the detrimental impact to security caused by an increased attack surface, which would allow for more directed denial-of-service attacks or even worse. The serving container reads from the processed data store and truncates it to what is relevant to an incoming user query.

The key factor during the rescue operations is the time, both the traceability and the synchronicity. The holdover - the useable time after losing verification of time is critical; as during a major emergency the EMS response time might not be ideal. To keep the synchronization between devices at an accurate level and take into account traceability NTP (network time protocol) is utilized within the system. The backend server handles disciplining local clocks to the verified atomic clocks, which makes them a Stratum 2 server. The primary NTP server is operating in Guardian mode. The backed server containers are synchronised to the local Guardian that puts them to Stratum 3. However, as they are at the same physical computer, they can also take reference from the system hardware clock, which is maintained by independent methods. Therefore it makes all local clocks equivalent to Stratum 2. The demo system is synchronised with NPL (National Physical Laboratory) and sanity checks the pooled NTP servers and Google's smear timeservers. Despite the instability of the containers inside the virtual machines, the entire system remains disciplined to Stratum 2 by the physical HWRTC (Hamilton-Wentworth Real-Time Control) as HWRTC are not installed on the Raspberry Pis.

5.1 Networking and Software

The key component of the backend server is pfsense, which is an open source, FreeBSD based software solution; primarily it is utilised as a dedicated firewall and/or router for a network. In the particular case of the proposed solution the main responsibilities of pfsense are operating as a firewall, NTP server, recursive DNS64 server and router for the purposes of the backend server; also it can be utilized as a monitoring (packet sniffer) to analyse network performance. Additionally pfsense is using custom routes, so all of the IPv4 leakages are routed to a TAYGA (user-mode stateless NAT64 implementation) server container, so that all of the IPv4 packages can be handled by it. TAYGA is setup as a NAT64 server operating on a 10.0.0.0/8 IPv4 private address space and the RFC6052 2.1 well-known IPv6 prefix 64:ff9b::/96. In the production setup, recursive DNS which is hooked to the root DNS servers, is utilised. Also it is useful to mention that currently pfsense does not support NAT64 and DNS64. According to pfsense changelog, which suggests TAYGA with the support of DNS64 will be added in the next version. The DNS server of the demo system is utilizing the Google public DNS64 service.

BGP (border gateway protocol) is handled on the ISP's remote server, as the demo system is designed to be portable and can be demonstrated in any location. The IPv6 is piped through a VPN from the project's ISP (Fluffyyy) to the pfsense (Guardian) . The ISP is set up as a static IPv4 VPN server, which is connected to the upstream provider (Hurricane Electric) at Equinix London LD8; that allows guardian to connect to the IPv6 Internet. Physically it is pure mesh topology and from the perspective of an IPv6 network protocol it is a bus topology. For the purposes of the proposed solution Proxmox clusters handles the deployment and hardware resource allocation and high availability Open vSwitch may be utilised for handling of networking. Mosh is used due to the likelihood of unstable operation during an emergency.

5.2 System Operation

All of the system's function can be described using the steps in the following sequence:

i. Beacon from mobile device broadcast is captured for a time window.
ii. Captured packet is encrypted.
iii. Encrypted data block is armoured with unicode character r, which helps to delimit the data at later stages.
iv. Encrypted and armoured data blocks are transmitted over IPFS pubsub.

At the backend server the following operations are conducted:

i. Unicode armouring is removed.
ii. GPG (GNU Privacy Guard) data block is decrypted.
iii. Data is verified (OK attribute is set to true and signed by a known source).
iv. Data is collected, analysed and formatted.
v. Data is offered up to BigchainDB via API.
vi. Loop is operating until no more blocks are left.

User is accessing the data store:

i. User selected specific time frame.
ii. Data is collected.
iii. Needed data from a reference data store is collected.
iv. Scanned data is compared with data from a reference lookup table.
v. Indoor location is outputted.

The lookup tables contain locations and the expected RSSI values. All the operations of the system are done within two scripts. The first script is operating within Raspberry Pis. In order to avoid stressing Raspberry Pis, Zsh (Z shell) environment has been chosen by the author. The script is responsible for pacing the devices, as it is necessary to avoid network failure due to the Raspberry Pis inability to operate stably with a noisy mesh network. The next steps are BLE raw frame collection and passing for encryption and signing by GPG. The next steps include armouring with Unicode character IPFS and passing to next Python script which is operating within the backend server. It is responsible for unarmouring, decryption, collation, analysis and formating of the data.

5.3 Applied Security Measures

Firewalls with various complementary abilities have been applied to onion the network. The first line of the network defence is the pfsense firewall with rules crafted in accordance with providing positive rights for acceptable packets. HFSE (Hierarchical Fair Service Curves) and stateful packet inspection are utilised by pfsense to bear the brunt of any attack. As a measure of security, the NDP (neighbour discovery protocol) table in pfsense is monitored to catch extraneous devices on the network. Reverse proxy (Nginx) technique is utilised for BigchainDB purposes in order to provide IPv6 compatibility, ease of use and security, as it rate limits BigchainDB from the open Internet. Besides using strong passwords as an option for increasing the level of authentication security the followings have been implemented: HMAC SHA-1 for physical authentication, TOTP (Time-based One-Time Password), the requirement to use authentication smart card, the demo uses a GPG authentication card. To prevent the use of easily predictable keys and key clash, custom moduli files have been created. Based on hardware limitations, parameters of operationally suitable cryptographic keys have been selected, namely based on RSA. NTP authentication and encryption is also utilised to prevent the possibility of timestamps to be tampered with, as its accuracy is crucial for the aims of emergency management. Isolated OvS (open virtual switch) is utilised to completely isolate and give privacy to processing and serving nodes. The last line of the network defence is UFW (uncomplicated firewall) and firewalls with custom rules utilised in Raspberry Pis, Valhalla (hypervisor) and CTs (LXE containers), which is used to allow the actions that are only whitelisted. That can be considered as an ancillary in case of pfsense protection failure. All Web GUIs utilised in the project are assigned an SSL certificate, which means that full HSTS (HTTP Strict Transport Security) can be operated.

6. Discussion

Utilisation of a building's Wi-Fi infrastructure in case of normal, non-emergency situation should be utilised, with the mesh network acting as a fallback. The software limitations of Raspberry Pis, as an ARM64hf platform has limited binary capabilities and many software applications are not ported well for this platform. For example, for the purposes of this project it has been planned to utilize BigchainDB, but as it requires MongoDB, which only an older version only is supported by Raspbian, it was hence not feasible to continue using this approach.

Critically evaluating the structure of the network, the single point of failure will be the central Raspberry Pi. For the future implementation and real deployment - multiple central Raspberry Pis will be utilized to avoid this single point of failure. In case of failure of one of the central devices, the IPFS swarm will be automatically adjusted and will survive the changes; the data will still then be able to reach a remote server.

Additionally testing of the system in a strenuous environment might be needed to get more realistic results and determine if the solution is efficient for the purposes of emergency management.

The second approach of the project, which is based on utilising a mobile device as a scanner requires more testing as well. As the results vary from the complexity of the environment and the theoretical approach, it should not be blindly trusted - as it may lead to issues and inaccuracies during people localisation in case of emergency.

A GUI solution must be adopted and in fact offered, this will provide ease of use and monitoring of database content and help the emergency services to interact with the sytem and hence locate people more effectively. It is envisioned that software like processing can be utilised. This will allow monitoring to be in graphical format (floor plans); additionally RSSI values will be converted to human understandable format by utilising mathematical equations and will be provided in distance format (metres).

7. Conclusion

This paper documents a BLE people locating system which fully supports IPv6 and legacy technology and which also exceeds the security standards and provides data management efficiency.

The project has a potential for utilisation in emergency management. The low total cost of the hardware components can be considered as beneficial; additionally software applications with open-source licences is advantageous in terms of budget saving and ability to customise software according to the requirements of the project

Acknowledgements: Many thanks to Dr Georgia Sakellari, Dr Avgoustinos Filippoupolitis and fluffyyy (colleague and ISP).

References

[1] Hat, R. (2017), "What is open source?", Available at: https://opensource.com/resources/what-open-source. (Accessed: 13/10/2017)

[2] Electronics, F. (2014), "Bluetooth Low Energy Modules, Solutions and Applications - Bluetooth LE, BLE", Available at: https://www.youtube.com/watch?v=AIHpSCYOQNI. (Accessed: 09/10/2017)

[3] Lester, S. (2015), "The Emergence of Bluetooth Low Energy | Context Information Security", Available at: https://www.contextis.com/blog/the-emergence-of-bluetooth-low-energy. (Accessed: 17/11/2017)

[4] Das, P. (2016), “Developing Beacons with Bluetooth® Low Energy (BLE) Technology”, Available at: https://www.slideshare.net/PallaviDas6/developing-beacons-with-bluetooth-low-energy-ble-technology-61620148.

[5] Argenox (2017), “Powering Wireless and Bluetooth LE Products with Batteries”, Available at: http://www.argenox.com/bluetooth-low-energy-ble-v4-0-development/library/powering-ble-batt.

[6] Alexandru, G. B. (2014), “A view on Bluetooth Low Energy stack roles | NXP Community”, Available at: https://community.nxp.com/thread/332319. (Accessed: 09/10/2017)

[7] Laird Technologies Wireless Connectivity Blog (2015), “An Overview of Addressing and Privacy for Laird’s BLE Modules”, Available at: http://www.summitdata.com/blog/overview-addressing-privacy-lairds-ble-modules.

[8] Babu, P. (2016), “10 Airports Using Beacons to Take Passenger Experience to the Next Level”. Available at: https://blog.beaconstac.com/2016/03/10-airports-using-beacons-to-take-passenger-experience-to-the-next-level.

[9] Mbed (2015), “Understanding the different types of BLE Beacons”, Available at: https://os.mbed.com/blog/entry/BLE-Beacons-URIBeacon-AltBeacons-iBeacon. (Accessed: 18/11/2017)

[10] Estimote (2017), “What is Eddystone? - Estimote Developer”, Available at: https://developer.estimote.com/eddystone.

[11] Palumbo F., Barsocchi P., Chessa S. and Augusto J. C., “A stigmergic approach to indoor localization using bluetooth low energy beacons”, In: AVSS 2015 - 12th IEEE International Conference on Advanced Video and Signal Based Surveillance (Karlsruhe, Germany, 25-28 August 2015). Proceedings, article n. 13. IEEE, 2015.

[12] Chandel, V., Ahmed, N., Arora, S. and Ghose, A. (2016) “InLoc: An end-to-end robust indoor localization and routing solution using mobile phones ad BLE beacons”, 2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN). 4-7 Oct. 2016.

[13] Gao, V. (2015), “Proximity And RSSI | Bluetooth Technology Website”, Available at: https://blog.bluetooth.com/proximity-and-rssi. (Accessed: 14/10/2017)

[14] Avgoustinos Filippoupolitis, William Oliff and George Loukas, “Bluetooth Low Energy based Occupancy Detection for Emergency Management”, 15th International Conference on Ubiquitous Computing and Communications (IUCC), Granada, Spain, 14-16 Dec. 2016.

[15] Lin X.Y., Ho T.W., Fang C.C., Yen Z.S., Yang B.J. and Lai F., “A mobile indoor positioning system based on iBeacon technology”, Proceedings of the 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC); Milan, Italy. 25–29 August 2015; pp. 4970–4973.

[16] Antevski, K., Redondi, A., Pitic, R. (2016), “A hybrid BLE and Wi-Fi localization system for the creation of study groups in smart libraries”, Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7543928.

[17] Kriz, P., Maly, F. and Kozel, T. (2016), “Improving indoor localization using bluetooth low energy beacons”, Mobile Information Systems, 2016.

[18] Rius, R. M., Talavera, G. and Carrabina, J. (2012), “Developing and study of wearable and flexible antennas for Body Area Networks working under extreme conditions”, 15th Int Symp on Antenna Technology and Applied Electromagnetics. 25-28 June 2012.