Seguridad y gestión de una red de beacons

Guillermo García Escoriza

Resumen—El presente proyecto ha consistido en el diseño, gestión e implementación de una red de beacons con el fin de ser utilizada como medio de localización a través de una aplicación Android. Esta aplicación muestra datos de interés al usuario con respecto a la zona en la que se encuentre. Este proyecto es aplicable a un gran número de contextos, desde publicitar ofertas en un centro comercial hasta guiar a los visitantes de un hospital a sus respectivas habitaciones. Se ha implementado, además, un sistema de seguridad que oculta la identidad de los beacons, dificultando en gran medida cualquier intento de suplantación de estos dispositivos. Para llevar a cabo el sistema descrito, se ha tenido que configurar una red de beacons Bluetooth, programar una aplicación móvil para Android, implementar un servidor en línea y aplicar el sistema de seguridad de beacons Eddystone-EID.

Palabras clave—Beacon | Eddystone | Bluetooth Low-Energy (BLE)

Abstract—The following project consists in the design, management and implementation of a network of beacons with the purpose of being used as a real-time location system through an Android application. The application offers data of interest to the user due to the area where he is located. This Project has a large number of applications, from advertising offered in a shopping center to guiding visitors in a hospital to their respective rooms. It has also been implemented a security system that hides the identity of the beacons, greatly hindering any attempt of hijacking or supplanting the devices. To carry out the described system, we have configured a network of Bluetooth beacons, programed a mobile application for Android, implemented an online server and applied the beacon security system known as Eddystone-EID.

Index Terms— Beacon | Eddystone | Bluetooth Low-Energy (BLE)

1 Introducción

LOS beacons se inventaron con el objetivo de crear una nueva forma de interacción entre el mundo físico y el digital, dando a objetos y lugares la potestad de comunicarse con usuarios cercanos. Esta tecnología ha sido aplicada en multitud de contextos y cada vez es más fácil toparse con servicios que la utilizan para mejorar su servicio al cliente. La Escuela de Ingeniería de la UAB pretende aprovechar esta tecnología con el fin de ofrecer a sus alumnos un método de localización y guiado a través de los pasillos del edificio. Disponiendo al principio de tan solo dos beacons sin configurar, se ha conseguido desarrollar un sistema de localización a través de una red de beacons mediante una aplicación móvil, implementando también una capa de seguridad que los protege frente a posibles intentos de suplantación. Siento un gran interés por el mundo de la domótica y la ciberseguridad, por lo que este proyecto me ha ofrecido una oportunidad excelente para poder expandir mis conocimientos en esos ámbitos de la informática.

- *E-mail de contacto: guillermo.garciaes@e-campus.uab.com*
- *Mención realizada: Ingeniería de Computadores.*
- *Trabajo tutorizado por: Marta Prim (Microelectrónica y sistemas electrónicos)*
- *Curso 2017/18*

Este documento describirá el proceso de diseño, desarrollo e implementación este sistema, y se explicará con detalle qué son y cómo funcionan los beacons, así como las aplicaciones actuales de esta tecnología. Seguidamente, definiremos este proyecto y los objetivos que se pretenden cumplir.
Detallaremos cada una de las etapas de desarrollo y terminaremos con las conclusiones extraídas a lo largo de todo el proceso, explicando también los obstáculos y problemas encontrados.

2 Tecnología Beacon

Los beacons consisten en dispositivos de pequeño tamaño que emiten un mensaje broadcast periódicamente. La tecnología beacon permite a smartphones, tablets y cualquier otro dispositivo con compatibilidad Bluetooth Low Energy realizar acciones cuando se encuentren cerca de un beacon. Estos dispositivos transmiten un identificador, conocido como Universally Unique Identifier (UID), que puede ser utilizado para determinar la posición física del dispositivo, monitorizar la actividad de usuarios o activar acciones basadas en la localización del dispositivo.
Se han implementado en muchos y muy diferentes contextos, la mayoría de ellos con el objetivo de difundir información sobre un punto de interés específico, como

podría ser dando los horarios de una parada de autobús o datos sobre una escultura en un museo [2]. Este tipo de aplicaciones se asemeja a la tecnología geopush [3], basada en GPS, pero en este caso con menor consumo energético y mejor precisión.
Uno de los puntos fuertes de esta tecnología es su uso como localizadores dentro de entornos cerrados, algo fuera del alcance para la tecnología GPS. El receptor del mensaje puede aproximar su posición relativa con respecto al beacon, siendo fácil ubicarlo en un mapa.
De esta forma, si se instala una red de beacons en un entorno controlado, se puede seguir la posición de los usuarios en todo momento. Lo que diferencia a las balizas bluetooth del resto de tecnologías con capacidad de localizar físicamente a un individuo es el hecho de que las balizas se comunican en una sola dirección, haciendo que se dependa de una aplicación, instalada en el dispositivo receptor, capaz de procesar ese mensaje y estimar la posición del usuario.

2.1 Hardware

La mayoría de beacons están compuestos por una CPU, un chip emisor de radiofrecuencia Bluetooth y una fuente de alimentación, comúnmente un juego de pequeñas baterías de litio de botón [4]. Aunque los nuevos modelos incorporan un chip con capacidad de Bluetooth Low Energy, los primeros diseños solo podían trabajar con el protocolo de Bluetooth clásico, requiriendo un consumo considerable de energía.
Existen actualmente tres familias populares de chips de radiofrecuencia Bluetooth; la CC254x, de Texas Instruments; la DA14580, de Dialog y la nrf51822, de Nordic. Estas compañías ofrecen circuitos electrónicos estándar y diseños de placas impresas para que las empresas fabricantes de beacons puedan utilizarlos en sus productos. Aunque distintos modelos se beacons compartan el mismo tipo de chip Bluetooth, pequeñas diferencias en su implementación, gestión energética, tipo de conectores o su toma a tierra pueden causar pérdidas de energía y ruidos en la señal, por lo que la calidad de la señal del beacon depende más de la implementación del chip Bluetooth que del chip en sí mismo [5].
El alcance de señal de un beacon ronda de los 70 metros en beacons regulares, hasta los 450 metros en beacons de largo alcance [6].
Los 2.4 GHz de frecuencia con el que los beacons se comunican, sin embargo, puede verse bloqueado o afectado por elementos como la carcasa del dispositivo, la batería o el propio circuito integrado. La antena emisora de la señal, que se encuentra adherida al circuito integrado, puede hacer también que el rango del alcance de los mensajes varíe en función de la orientación del beacon [7].
Como ya se ha comentado, las baterías de botón son el método más común para alimentar estos dispositivos. Estas baterías consisten en células de iones de litio y ofrecen desde 240 mAh hasta 1000mAh, aunque también hay modelos de beacons con compartimento para juegos de baterías AA [8].
Otros beacons, en cambio, se alimentan de una fuente externa mediante una toma de corriente o un puerto USB. Ofrecen la ventaja de que no debe controlarse el estado de sus baterías, pero deben poseer una fuente de alimentación cercana a la que conectarse para funcionar. Se pueden encontrar beacons en multitud de formas, colores y tamaños, incluyendo también sensores como termómetros y acelerómetros para expandir sus posibles usos.
El objetivo principal de ofrecer un rango tan amplio de modelos diferentes es el de adaptar el uso de esta tecnología a cualquier contexto, por lo que ahora existen desde beacons del tamaño de una tarjeta de crédito para poder llevarlos siempre contigo, hasta beacons impermeables y sumergibles para contextos industriales.

2.2 Software

La tecnología Bluetooth mediante la cual se comunican los beacons es la Bluetooth Low Energy [9].
Esta versión de la tecnología Bluetooth fue diseñada y comercializada por Bluetooth Special Interest Group, cuyo objetivo era ofrecer un método de comunicación por radiofrecuencia con un consumo de energía reducido, pensado para aplicaciones relacionadas con el fitness, la seguridad, la salud y los beacons, ya que estas suelen depender de baterías y el consumo energético es un factor crucial.
El Bluetooth Low Energy es capaz de reducir considerablemente ese consumo y mantener un rango de alcance similar al del Bluetooth original.
Existen diversos protocolos de comunicación Bluetooth para beacons, pero los más comunes son el iBeacon y el Eddystone.
iBeacon [10], desarrollado por Apple y presentado en el 2013, consiste en un protocolo de comunicación para beacons con compatibilidad tanto para sistemas operativos iOS como para Android, aunque su versión nativa solo se encuentra en iOS. Permite transmitir mensajes broadcast con el identificador único del beacon.
Eddystone [11], desarrollado por Google, es otro protocolo de comunicación para beacons que ofrece nuevas y mejoradas funcionalidades. Es compatible con cualquier tipo de plataforma que soporte comunicaciones Bluetooth Low Energy, por lo que se puede utilizar tanto desde Android como iOS.
Además, es capaz de transmitir mediante broadcast 4 tipos de mensajes diferentes [12]:

- Eddystone-UID: Identificador único de 16 bytes, compuesto por 10 bytes de espacio de nombres y 6 bytes de instancia. La porción del espacio de nombres puede ser utilizada para identificar el beacon según su grupo y tipo, indicando por ejemplo su uso o funcionalidad. La porción de instancia, por otra parte, identifica al beacon dentro de ese grupo.
- Eddystone-EID: Identificador efímero cifrado que cambia periódicamente. Este identificador deberá ser resuelto remotamente a través de la plataforma en la que el beacon se registró.
- Eddystone-TLM: Información telemétrica sobre

el estado del beacon en sí, como el voltaje de la batería, la temperatura del dispositivo o un conteo de los mensajes emitidos.

- Eddystone-URL: consiste en una URL codificada y comprimida. Esta URL, al ser decodificada, podrá ser accedida a través de cualquier navegador web. La tecnología del Google's Physical Web Project [13] se basaba en este tipo de mensajes para su funcionamiento.

2.3 Estado del arte

Uno de los primeros usos que se les dio a la tecnología de beacons fue en establecimientos de Estados Unidos, donde cadenas como Macy [14] recurrían a beacons para anunciar ofertas entre sus clientes. Estos recibían mensajes en sus teléfonos móviles cuando se encontraban cerca de ciertos productos.

Los beacons también han alcanzado el mundo de la hostelería [15] y se utilizan beacons para ofrecer información actualizada sobre el hotel, como actividades, ocupación en el restaurante, etc. Algunos museos han empezado a instalar redes de beacons para darles una función similar; ofrecer información de las obras a sus visitantes.

Por ahora, el principal enfoque que se le ha dado a esta tecnología ha sido la de marcadores de ruta y se le está buscando utilidad en el ámbito del turismo, pero se espera que se le encuentre nuevos usos dentro del hogar, añadiendo otro componente más al mundo de la domótica.

2.4 Beacons utilizados para este proyecto

Para este proyecto, se han utilizado beacons IBKS 105 [16], de la compañía Accent Systems. En la figura 1 y 2 podemos ver sus medidas y aspecto real.

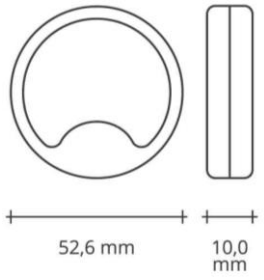

Figura 1: Medidas del IBKS 105 [17]

Figura 2: Fotografía del IBKS 105

Los beacons IBKS 105 son, oficialmente, los primeros beacons compatibles con los protocolos de comunicación iBeacon™ y Eddystone™ al mismo tiempo. Su firmware es actualizable mediante el air Eddystone Configuration GATT Service, previniendo su obsolescencia a nivel software. Sus baterías, con una capacidad de 1000 mAh, consisten en una pila CR2477 que durará una media de 30 a 40 meses, pero puede variar según la cantidad de mensajes enviados simultáneamente y la frecuencia de emisión de estos. Su chip de radio Bluetooth Low Energy es un nrf51822 de Nordic Semiconductors.

Tienen un alcance efectivo de unos 50 metros, pero puede variar según la orientación y los obstáculos entre el beacon y el usuario.

Disponen de una capa adhesiva en su lado trasero para poder ser adheridos sobre cualquier superficie. Pueden operar en un rango de -30 a +60 grados centígrados, pero es recomendable evitar cambios bruscos de temperatura para mantener la batería en buen estado. Existe la versión sencilla y la impermeable, que permite instalar estos beacons al aire libre o en zonas húmedas.

Nosotros hemos utilizado la versión no impermeable, pues se pretende que este sistema sea instalado en entornos cubiertos y secos. Su precio ronda los 12 euros por unidad, por lo que se deben intentar repartir de la forma más útil y efectiva posible con el fin de minimizar gastos.

3 PROYECTO ACTUAL

3.1 Descripción

Este proyecto consiste en el diseño, desarrollo e implementación de un sistema de localización mediante una red de beacons y una aplicación móvil.

Además, es de suma importancia añadir un sistema de seguridad para proteger los beacons de ser suplantados. Para conseguirlo, se ha dividido el sistema en 3 módulos:

- Red de beacons: Infraestructura de balizas Bluetooth. Cada uno de los beacons transmitirá un mensaje que será utilizado para identificar el beacon y, por ende, la zona en la que se encuentra el beacon y el receptor.
- Aplicación móvil: Recibe las identificaciones de los beacons y las envía al servidor. La respuesta de este indicará qué información debe mostrar la aplicación por pantalla. Su finalidad es la de indicar al usuario en qué zona se encuentra
- Servidor: Recibe identificadores de beacon y responde con un indicador de los datos que la aplicación debe mostrar.

La figura 3 muestra los distintos módulos de este sistema:

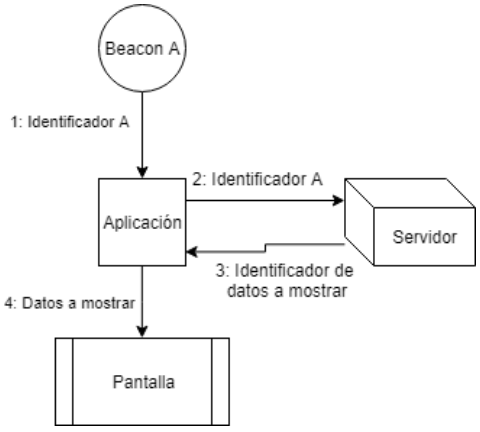

Figura 3: Diagrama de módulos del sistema

1. Un beacon emite por broadcast su identificador y este es recibido por la aplicación móvil.
2. La aplicación reenvía este identificador al servidor.
3. El servidor responde con el identificador de los datos a mostrar.
4. La aplicación muestra por pantalla la información correspondiente.

La seguridad reside en el tipo de identificador que enviarán los beacons. Se comunicarán mediante el protocolo Eddystone™ y enviarán mensajes Eddystone-EID [18]. Los mensajes Eddystone-EID consisten en identificadores dinámicos, es decir, que cambian periódicamente, imposibilitando de esa forma la suplantación de las balizas.

3.2 Objetivos

El objetivo a largo plazo es dotar a los visitantes y estudiantes de la Escuela de Ingeniería de la UAB de un sistema de guiado para aulas y despachos en la Escuela de Ingeniería de la UAB.
Los visitantes tendrían una fuente de información a tiempo real del lugar en el que se encuentran, mejorando su orientación y facilitando considerablemente la interacción entre los profesores y los alumnos. La información ofrecida a través de la aplicación consistiría en:

- Planta actual: La planta en la que se encuentra el visitante.
- Sección actual: Nombre de la sección en la que se encuentra el visitante. Por ejemplo: Despachos de química.
- Despachos circundantes: Una lista de los despachos más cercanos al visitante, indicando también sus profesores y un enlace a sus perfiles dentro de la web de la universidad.

Los beacons serían repartidos a lo largo de los despachos de la Escuela de Ingeniería de la UAB, adhiriéndose al techo cada 4 despachos y en las puertas de entrada y salida de los pasillos tal y como muestra la figura 4.

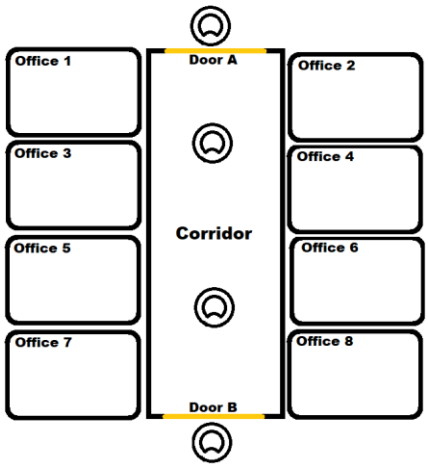

Figura 4: Diagrama de módulos del sistema

Con este sistema, se espera que, en un espacio de 6 a 9 meses desde su implementación, se obtengan los siguientes resultados:

- Reducir el tiempo de trayecto entre cualquier punto de la escuela y los despachos de los profesores en un 15%.
- Mejorar la interacción entre profesores y alumnos.
- Incrementar el rango de difusión de horarios de visita, así como de cualquier información sobre incidencias o novedades al respecto, reduciendo el número de consultas en recepción con respecto a horarios de visita e indicaciones un 15%.
- Alcanzar una alto índice de popularidad entre el alumnado, recibiendo 60 visitas diarias a la aplicación.

Como objetivos técnicos, se propusieron los siguientes:

- Disponer del prototipo de un sistema de guiado por beacons en un plazo de 5 meses.
- Proteger los beacons frente a cualquier intento de suplantación.

3.3 Planificación

Este proyecto se ha enfocado mediante una metodología basada en sprints de 15 días, afrontando cada una de las tareas individualmente y testeándolas antes de progresar con la siguiente. Se ha dividido el desarrollo de este sistema en 4 etapas, cada una de ellas con sus tareas respectivas, de la siguiente forma:

- Configuración beacons:
  - Aprendizaje del funcionamiento de los beacons
  - Configuración mediante su aplicación oficial
- Desarrollo aplicación:
  - Aprendizaje de desarrollo de aplicaciones móvil
  - Testeo y realización de un “Hello world” con los beacons

    - Creación de una User Interface sencilla
    - App funcional pero con procesamiento de EID local
- Implementación servidor:
    - Contratación del servidor
    - Aprendizaje del funcionamiento de servidores en línea
    - Implementación de un servidor
    - Conexión entre la aplicación y el servidor
    - Conexión con la API de Google para la traducción de EIDs
- Pruebas y documentación:
    - Testeo
    - Análisis de resultados

Durante el transcurso del proyecto, se ha ido documentando cada una de las fases y, al tratarse de un trabajo de final de grado, se ha preparado una presentación Power Point para exponerlo al público. Aunque se han sufrido complicaciones y obstáculos que han ido retrasando la planificación inicial, se han conseguido realizar todas las tareas propuestas.

4 DESARROLLO

4.1 Configuración beacons

Los beacons fabricados por la compañía Accent Systems permiten ser gestionados mediante la aplicación IBKS Config Tool [19]. Esta aplicación puede ser utilizada para escanear los beacons cercanos, programarlos y actualizar su firmware.

Para implementar el sistema de seguridad mencionado anteriormente, los beacons deben ser registrados en una plataforma compatible con Eddystone-EID. En nuestro caso, se han registrado en un proyecto de la Google Cloud Console [20] con la Google Proximity Beacon API [21] activada mediante la aplicación IBKS Config Tool.

Seguidamente, se han configurado los beacons para retransmitir un identificador efímero con un periodo de rotación de 17 minutos, asignándole una clave a cada uno de ellos con la que cifrarán sus identificadores. Se han elegido 17 minutos porque es el valor mínimo de rotación configurable con los Beacons IBKS 105 desde su plataforma oficial.

La clave de cifrado del sistema de seguridad EID solo es conocida por la plataforma de Google y el propio beacon. De esta forma, nuestros beacons emitirán un identificador efímero que cambiará cada 17 minutos, haciendo que cualquier usuario malicioso que esté monitorizando la red en busca de identificadores dinámicos, tan solo encuentre datos aleatorios sin sentido.

Para evitar que los beacons sean reconfigurados por un tercero una vez hayan sido instalados, existe una opción denominada modo conectable.

Los beacons se adquieren, por defecto, con el modo conectable activado. En este modo, los beacons pueden ser configurados utilizando las herramientas de desarrollador disponibles en el mercado.

Una vez finalizada su configuración, se debe desactivar el modo conectable, cosa que bloqueará el acceso a la configuración del beacon. Para volver al modo conectable y realizar algún cambio a la configuración, se debe extraer la pila del dispositivo y volverla a colocar. De esta forma, el beacon se mantendrá conectable durante un periodo de tiempo establecido, permitiendo reconfigurarlo.

4.2 Aplicación móvil

La aplicación móvil tiene 4 tareas; monitorizar las señales Bluetooth en busca de identificadores efímeros, decidir si debe desechar o procesar ese identificador, conectarse con el servidor para conocer qué datos debe mostrar por pantalla y, definitivamente, proyectar la información correspondiente.

Para programar la monitorización de señales Bluetooth se ha utilizado la librería AltBeacon [22]. Esta librería permite detectar beacons desde cualquier dispositivo con una versión de Android posterior a la 4.3 y compatibilidad con Bluetooth Low Energy. Además, se puede estimar la distancia a la que se encuentran los beacons con bastante precisión, dando un fallo de 10 centímetros.

Utilizando esta librería, no solo contamos con una forma fácil de obtención del identificador de los beacons, sino también con una estimación de sus distancias con respecto al usuario.

Al arrancar la aplicación y activar el modo de escaneo, se comenzará a monitorizar el tráfico de radiofrecuencia Bluetooth en busca de mensajes con el formato EID. De esta forma, tan solo los beacons que emitan ese tipo de mensaje serán detectados y procesados.

Tras detectar un EID, se deberá decidir si se debe procesar y de qué forma, intentando minimizar el número de peticiones realizadas al servidor. Para ello, se considerarán los identificadores efímeros y las distancias del último beacon identificado.

En caso de que los identificadores sean diferentes y la distancia del nuevo sea menor que la del último, se realizará la petición al servidor y se mostrará por pantalla los datos del nuevo beacon. Si los identificadores son iguales, se actualiza la distancia a la que se encuentra ese beacon. Cualquier otra posibilidad es obviada y la aplicación no alterará los datos presentados.

La figura 5 muestra el diagrama de flujo del proceso de toma de decisiones de la aplicación.

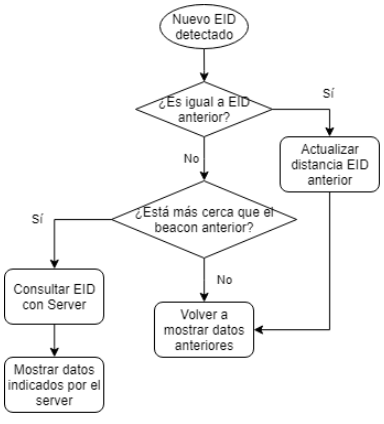

Figura 5: Diagrama de flujo del algoritmo de toma de decisiones

La información sobre las zonas contempladas en nuestro sistema se encuentra guardada dentro de la propia aplicación en forma de un diccionario, cuyas claves son los identificadores de zona y los valores, objetos con la siguiente información:

- Número de planta
- Nombre de sección
- ID de imagen

Las siguientes figuras muestran el aspecto de la pantalla de bienvenida de la aplicación, en la figura 6, y la pantalla de datos, en la figura 7.

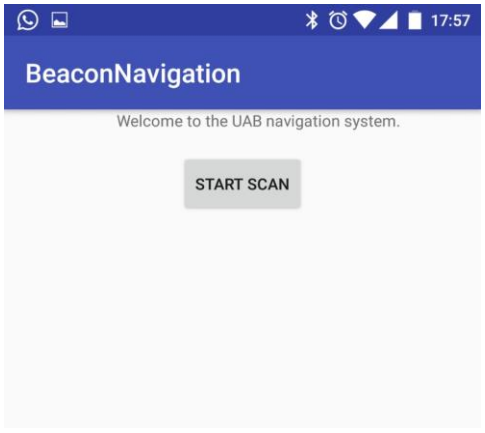

Figura 6: Pantalla de bienvenida de la aplicación

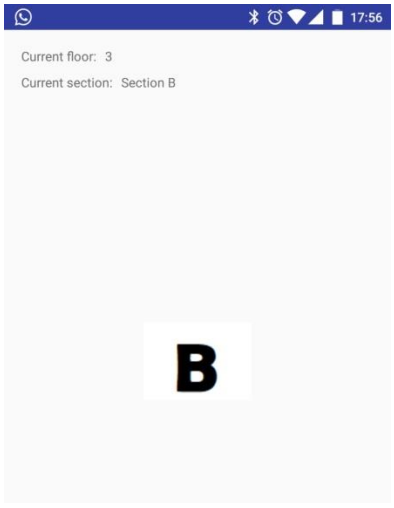

Figura 7: Pantalla de datos de la aplicación

Las consultas de EIDs con el servidor se realizarán como consultas HTTP GET, enviando en el parámetro "id" la EID del beacon a analizar. Tras cada consulta de EIDs con el servidor, se obtendrá un identificador de zona, es decir, la clave del diccionario asociada a la zona correspondiente, que servirá para saber qué datos han de ser mostrados por pantalla.
La aplicación móvil ha sido programada mediante el entorno de desarrollo integrado para el sistema operativo Android. La aplicación resultante consta de dos actividades; la actividad principal, que da la bienvenida al usuario y muestra un botón para iniciar el escaneo; y la actividad ranging, que rastrea EIDs a través de Bluetooth y muestra los datos correspondientes por pantalla.
El principal obstáculo durante esta etapa ha sido el aprendizaje de desarrollo de aplicaciones móviles. Se ha tenido que visualizar tutoriales y leer diversos manuales con tal de poder realizar una aplicación medianamente funcional y estética.

4.3 Servidor

El servidor en línea ha sido implementado como un Java servlet subido a la plataforma Amazon Web Services [23]. Utilizando una cuenta gratuita, esta plataforma permite hospedar una aplicación web sin coste alguno, siempre y cuando no supere una cantidad de tráfico establecido. Para este proyecto, y a modo de prueba de concepto, esta oferta ha sido más que suficiente.
El servidor tiene la tarea de responder a las peticiones HTTP GET realizadas por la aplicación móvil. Para ello, dispone de una lista de relaciones UID-Identificador de Zona que usaremos para saber en qué zona se encuentra el beacon detectado y, en consecuencia, qué información se debe mostrar.
Con cada petición, el servidor se conectará con la API de Google (explicado a continuación) para obtener el identificador estático y se cotejará con la lista de relaciones UID-Identificador de Zona. Si el EID es válido, se responderá a la petición con el Identificador de Zona correspondiente.

4.4 Seguridad

Las balizas han sido configuradas para emitir un identificador dinámico que, por sí solo, no nos da ninguna información respecto al beacon que lo ha emitido. Para poder conocer la identidad real del beacon y mostrar por pantalla los datos correspondientes, este identificador debe ser traducido. El servidor debe ser capaz obtener el identificador estático del beacon a partir del identificador dinámico que la aplicación le habrá transmitido.
La API de Google en la que se han registrado los beacons ofrece ese servicio; se le pueden realizar peticiones mandándole la identificación dinámica y esta responderá con la identificación estática.
Estas peticiones, al estar solicitando información protegida, exigen una autenticación para demostrar que se trata de una interacción autorizada por el administrador del sistema.
Si un usuario malicioso lograse recopilar los identificadores dinámicos de nuestros beacons, no tendría forma de traducirlos sin identificarse antes en la API de Google, por lo que, para él, esos identificadores no serían más que números aleatorios.
Las APIs de Google utilizan el protocolo OAuth 2.0 [24] para gestionar las autorizaciones y autenticaciones. El protocolo OAuth 2.0 [25] permite a una aplicación externa acceso limitado a un servicio HTTP, en este caso la API de Google de gestión de Beacons.
Para obtener autorización mediante el protocolo de OAuth 2.0, debe realizar una autenticación de 3 pasos; primero, se obtienen las credenciales OAuth 2.0 de la

Google API Console; segundo, se solicita un token de acceso a al Google Authorization Server; Tercero, se extrae ese token de la respuesta y se adjunta a todas las peticiones que se realicen a la API de Google a la que se pretenda acceder.
Los token de sesión tienen un tiempo de vida establecido y, cuando caduquen, se debe de obtener otro de nuevo desde el Google Authorization Server.
Con el fin de obtener un token de sesión, el propietario del recurso al que se quiere acceder, es decir, el administrador del proyecto en el que se han registrado los beacons, debe aprobar esta interacción de forma explícita suministrando sus credenciales de Google.
Realizar esa solicitud de forma manual a la API de Google mediante un navegador dirige a una página de log-in de Google, exigiendo el correo electrónico y la contraseña del administrador del servicio solicitado.
Esta mecánica imposibilita su uso en nuestro sistema, ya que las peticiones deben ser realizadas y automatizadas desde un servidor sin ningún tipo de intervención humana. Por suerte, OAuth 2.0 permite también autorizar a una aplicación externa acceso a este servicio HTTP mediante otro tipo de autenticación. En casos como el nuestro, nuestro servidor debe de probar su propia identidad con la API con el fin de acceder a la información restringida de nuestros beacons.
Para ello, se debe recurrir a una cuenta de servicio, que consiste en una cuenta de Google que pertenece a nuestra aplicación en lugar de pertenecer a un usuario. Nuestro servidor realizará las peticiones en nombre de esa cuenta de servicio y no será necesario ningún tipo de log-in.
Las cuentas de servicio se pueden crear desde la Google API Console, asociándolas directamente al proyecto en el que están registrados los beacons, y obtendremos una dirección de email, una identificación de cliente y, al menos, una pareja de claves pública y privada.
El servidor utilizará esas credenciales para autenticarse con el Google Authorization. Estas credenciales deberán ser transmitidas en un formato JSON Web Token [26] firmado criptográficamente con la clave privada e incluirán la ID de cliente de la cuenta de servicio.
Si las credenciales son correctas, Google nos responderá con el token de sesión con el que se podrán realizar el resto de peticiones a la API de Google.
En caso de que el token caduque, el servidor repetirá el paso inicial para obtener otro token actualizado.
La figura 8 muestra un esquema de este modelo de autenticación.

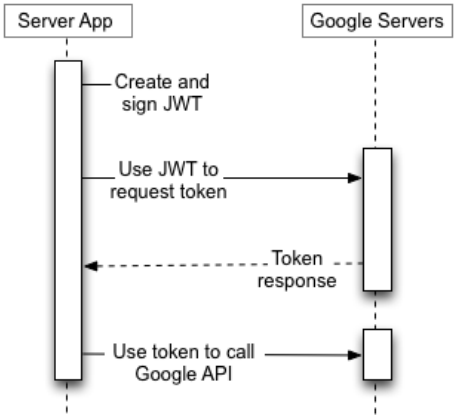

Figura 8: Modelo de autenticación OAuth 2.0 [27]

Para conseguir implementar este sistema de seguridad en nuestro proyecto, ha sido necesario recurrir a una gran cantidad de documentación y manuales de distintas fuentes. Se han encontrado muy pocos ejemplos de sistemas similares al de este proyecto, por lo que se ha acabado por entender su funcionamiento teórico y luego implementarlo lo mejor posible utilizando los conocimientos de java y redes adquiridos durante mis estudios, sin seguir ningún modelo o ejemplo.

5 CONCLUSIONES

Producto final

El producto final de este proyecto ha sido un sistema de localización mediante beacons Bluetooth, utilizando una aplicación específica y protegiendo los dispositivos de posibles intentos de suplantación.
Se han configurado una serie de beacons, se ha programado una aplicación Android, se ha implementado un servidor en línea y se ha configurado un sistema de seguridad para proteger a los beacons de ser suplantados.
El trabajar con una tecnología como esta, relativamente moderna todavía, ha supuesto un obstáculo a la hora de encontrar documentación y guías sobre cómo utilizarla. Por otro lado, se ha aprendido mucho sobre la realización de un proyecto desde cero, que abrace todas las facetas del ámbito de la informática y la ingeniería.
Se ha trabajado con dispositivos físicos, teniendo que considerar factores como su consumo energético, su integridad física, el ambiente, los materiales y hasta el color de los dispositivos en sí, con el fin de integrarlos lo mejor posible al entorno al que están destinados.
Se ha tenido que diseñar una infraestructura software multiplataforma, es decir, la aplicación móvil y el servidor, implementando sus métodos de comunicación. Se ha trabajado además en añadir seguridad al sistema, cifrando datos y gestionando autorizaciones y credenciales.
Por ello, este proyecto ha supuesto un desafío completo y difícil, lleno de obstáculos que se han tenido que superar uno a uno, aprendiendo con cada uno de ellos y, finalmente, obteniendo un resultado completo y satisfactorio.

Análisis de producto final

Este proyecto se ha evaluado en tres ámbitos diferentes: infraestructura del sistema, funcionalidades y su viabilidad.

- Infraestructura del sistema: Hemos conseguido crear un sistema de localización mediante beacons partiendo tan solo de una idea y dos beacons IBKS 105.
  Tanto la configuración de los beacons como la programación de la aplicación web y el servidor se han realizado con herramientas y aplicaciones públicas y gratuitas. Ha habido una ardua tarea de documentación y formación en ámbitos como el desarrollo de aplicaciones Android y protocolos de autenticación.
  El producto final es un sistema robusto y extensible, con potencial para ser utilizado en multitud de contextos, por lo que el resultado en este campo ha sido satisfactorio.
- Funcionalidades: Tal y como indica el título del proyecto, este se basaba en la seguridad y gestión de una red de beacons.
  Se ha conseguido proteger la identidad de los dispositivos beacon frente a posibles suplantaciones gracias al protocolo de cifrado de mensajes detrás del Eddystone-EID.
  Aún hay cabida para otras capas de seguridad, como cifrar las comunicaciones entre la aplicación y el servidor o proteger la aplicación móvil contra intentos de ingeniería inversa.
- Viabilidad: El resultado final de este proyecto pretendía ser testeado en entornos reales como la zona de despachos de la Escuela de Ingeniería de la UAB.

Objetivos cumplidos y dificultades encontradas

Se han cumplido los dos objetivos específicos, tanto el de disponer del prototipo de un sistema de localización mediante una red de beacons como el de proteger la infraestructura de balizas.
Se han encontrado diversas dificultades a lo largo de este proyecto, llevando a influir en la planificación inicial. La siguiente lista enumerará brevemente en qué han consistido, cómo se han solucionado y cómo han perjudicado a la planificación del proyecto:

- Aplicación de configuración de beacons oficial de IBKS incompatible con los teléfonos móviles disponibles:
  La aplicación ofrecida por Accent Systems para configurar sus productos no parecía funcionar en nuestros dispositivos móviles. Nos tuvimos que poner en contacto con la compañía y esta nos recomendó utilizar un teléfono móvil actualizado y con capacidades tanto de GPS como de Bluetooth.
  Solución: Adquisición de un teléfono móvil más moderno.
  Tiempo de retraso: 1 semana.
- Gestión de threads de la aplicación móvil:
  Al realizar conexiones al servidor desde el móvil de manera asíncrona, se perdía por completo la estabilidad de estos y la aplicación mostraba datos incorrectos.
  Solución: Replanteamiento del tipo de acceso a los datos críticos de la aplicación.
  Tiempo de retraso: 2 semanas.
- Implementación del sistema de seguridad:
  El trabajar con el protocolo de autorización OAuth 2.0, nos encontramos con enormes dificultades para comprenderlo e implementarlo en nuestro sistema.
  Solución: Lectura de toda la documentación posible.
  Tiempo de retraso: 2 semanas.

Líneas futuras

Aunque el funcionamiento general del sistema es correcto y se ha testeado en numerosas ocasiones bajo condiciones controladas, no se ha llegado a configurar para ser utilizado en un contexto real.
La aplicación móvil, aunque funcional, es sencilla y simple y no se encuentra preparada como para comercializada de cara al público.
Tampoco estamos del todo satisfechos con el tiempo de respuesta de la aplicación frente la detección de nuevos beacons, ya que tarda entre 10 y 20 segundos en actualizar la información a mostrar.
Como líneas futuras, se podrían establecer los siguientes objetivos:

- Mejorar la interfaz de la aplicación móvil implementando un diseño más elaborado.
- Modificar la estructura del sistema para que los datos de los beacons se guarden en el servidor en lugar de en la aplicación. Esto permitiría modificar, añadir o eliminar la información a mostrar sin tener que actualizar la aplicación, aumentando en gran medida la extensibilidad del sistema.
- Reducir el tiempo de respuesta implementando una caché en el servidor o en la propia aplicación.

BIBLIOGRAFÍA

[1] "Platform Overview | Beacons | Google Developers", May. 25, 2018. [En línea]. Disponible en: https://developers.google.com/beacons/overview
[2] "What are beacons? - Kontakt.io", Oct. 13, 2016. [En línea]. Disponible en: https://kontakt.io/beacon-basics/what-is-a-beacon/
[3] "What is GeoPush and why it matters? | Apollo Apps", Nov, 1, 2017. [En línea]. Disponible en: https://apolloapps.com/what-is-geopush-and-why-it-matters/
[4] Nick "The Hitchhikers Guide to iBeacon Hardware: A Comprehensive Report by Aislelabs (2015)", May. 4, 2015. [En línea]. Disponible en:

https://www.aislelabs.com/reports/beacon-guide/

[5] "The Affect of Beacon Processor Chip" Mar. 18, 2016. Disponible en: https://www.beaconzone.co.uk/blog/the-affect-of-beacon-processor-chip/
[6] "iBeacon - Wikipedia" Jun. 11, 2018. Disponible en: https://en.wikipedia.org/wiki/IBeacon
[7] "Beacon Orientation vs Range" Jul. 1, 2016. Disponible en: https://en.wikipedia.org/wiki/IBeacon
[8] "Beacon Battery Size, Type, Capacity and Life" Mar. 23, 2016. Disponible en: https://www.beaconzone.co.uk/blog/beacon-battery-size-type-capacity-and-life/
[9] "SIG INTRODUCES BLUETOOTH LOW ENERGY WIRELESS TECHNOLOGY, THE NEXT GENERATION OF BLUETOOTH WIRELESS TECHNOLOGY", Dic. 1, 2009. [En línea]. Disponible en: https://www.bluetooth.com/news/pressreleases/2009/12/17/sig-introduces-bluetooth-low-energy-wireless-technologythe-next-generation-of-bluetooth-wireless-technology
[10] "Getting Started with iBeacon", Jun. 2, 2014. [En línea]. Disponible en: https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf7
[11] "Eddystone format", Abr. 27, 2018. [En línea]. Disponible en: https://developers.google.com/beacons/eddystone
[12] Michael Ashbridge, "eddystone/protocol-specification.md", Abr. 14, 2016. [En línea]. Disponible en: https://github.com/google/eddystone/blob/master/protocol-specification.md
[13] "The Physical Web", May. 18, 2016. [En línea]. Disponible en: https://google.github.io/physical-web/
[14] Carlos Cabello, "9 usos reales para comprender qué son los beacons" Jul. 2016. [En línea]. Disponible en: https://www.nobbot.com/redes/9-usos-reales-comprender-los-beacons/
[15] Ausiàs, "Smart Hotel: Primera experiencia Beacon en hostelería en Barcelona", Dic. 31, 2014. [En línea]. Disponible en: https://kukoa.com/blog/apps/smart-hotel-primera-experiencia-beacon-en-hosteleria-en-barcelona
[16] "IBKS 105", Feb. 21, 2017. [En línea]. Disponible en: https://accent-systems.com/es/producto/ibks-105/
[17] "Plano Beacon",[En línea]. Disponible en: https://accent-systems.com/wp-content/uploads/size.jpg
[18] "Eddystone Ephemeral Identifier", Feb. 9, 2017. [En línea]. Disponible en: https://developers.google.com/beacons/eddystone-eid
[19] " iBKS Config Tool", Abr. 3, 2018. [En línea]. Disponible en: https://play.google.com/store/apps/details?id=com.accent_systems.ibks_config_tool&hl=es
[20] "Cloud Computing, servicios de alojamiento y APIs de Google Cloud", Ago. 8, 2016. [En línea]. Disponible en: https://cloud.google.com/
[21] "Proximity Beacon Overview", Feb. 9, 2017. [En línea]. Disponible en: https://developers.google.com/beacons/proximity/guides
[22] "Altbeacon Library", Nov. 9, 2014. [En línea]. Disponible en: https://altbeacon.github.io/android-beacon-library/index.html
[23] "AWS | Cloud Computing - Servicios de informática en la nube", May. 11, 2018. [En línea]. Disponible en: https://aws.amazon.com/es/
[24] "Using OAuth 2.0 to Access Google APIs" Abr. 20, 2018. [En línea]. Disponible en: https://developers.google.com/identity/protocols/OAuth2
[25] "The OAuth 2.0 Authorization Framework" Oct. 2018. [En línea]. Disponible en: https://tools.ietf.org/html/rfc6749
[26] "JSON Web Tokens" Abr. 26, 2018. [En línea]. Disponible en: https://jwt.io/
[27] "Esquema Autenticacion OAut 2.0", [En línea] Disponible en: https://developers.google.com/accounts/images/serviceaccount.png

Anexo A:
Planificación Inicial

12/03 - 25/03: Configuración beacons
-Aprendizaje del funcionamiento de los beacons
-Configuración mediante su aplicación oficial

26/03 - 09/04: Desarrollo aplicación
-Aprendizaje de desarrollo de aplicaciones móvil
-Testeo y realización de un "Hello world" con los beacons
-Creación de una User Interface sencilla
-App funcional pero con procesamiento de EID local

10/04 - 07/05: Implementación servidor
-Contratación del servidor
-Aprendizaje del funcionamiento de servidores en línea
-Implementación de un servidor
-Conexión entre la aplicación y el servidor

08/05 - 04/06: Pruebas y documentación.
-Instalación en el pasillo de la escuela de ingeniería
-Análisis de resultados

Anexo B:
Especificaciones IBKS 105:

- Dimensions: Ø52.6 x 11.3 mm
- Weight : 24g
- Core : Nordic nRF51822
- Radio Protocol: Bluetooth® Low Energy
- Distance Range: Up to 50m
- Battery: Coin Cell CR2477, 3V – 1000mAh
- Optional Sensors: Hall, Accelerometer
- Idle Current Consu-mption: 2.4µA
- Case material: ABS
- Case finish: Matte white
- Fixing method: Double side sticker
- Operating Temperature: -25 to +60ºC
- Storage Temperature: 0 to +35ºC
- Beacon Protocols: iBeacon, Eddystone
- Firmware Update: OTA (Over The Air)
- Certifications: CE, FCC, IC, Anatel