Trabajo Fin de Grado
Grado en Ingeniería Electrónica, Robótica y Mecatrónica

Diseño e implementación de un sistema de identificación de terminales móviles en un área basado en el código IMSI

Autora: Marta Julia López González de Quevedo

Tutor: Jesús Iván Maza Alcañiz

Dpto. Ingeniería de Sistemas y Automática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2021

Trabajo Fin de Grado
Grado en Ingeniería Electrónica, Robótica y Mecatrónica

Diseño e implementación de un sistema de identificación de terminales móviles en un área basado en el código IMSI

Autora:
Marta Julia López González de Quevedo

Tutor:
Jesús Iván Maza Alcañiz

Dpto. Ingeniería de Sistemas y Automática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2021

Trabajo Fin de Grado: Diseño e implementación de un sistema de identificación de terminales móviles en un área basado en el código IMSI

Autora: Marta Julia López González de Quevedo
Tutor: Jesús Iván Maza Alcañiz

El tribunal nombrado para juzgar el trabajo arriba indicado, compuesto por los siguientes profesores:

Presidente:

Vocal/es:

Secretario:

acuerdan otorgarle la calificación de:

El Secretario del Tribunal

Fecha:

Agradecimientos

Agradecer en primer lugar a mi tutor Iván Maza, así como a Adolfo, Guillermo y mis compañeros de 4i, por la paciencia y la oportunidad de realizar este proyecto.

A toda la gente que me llevo de estos cinco años, ya sea de la carrera, de la residencia o de bonitas casualidades. Por todos los momentos compartidos, por su ayuda, por las horas de estudio y las de no tanto estudio, por creer en mi y ayudarme a crecer. A Noelia y Carmen, por estar conmigo durante todo el proceso de realización de este trabajo.

En especial agradecer a mi familia, por su apoyo incondicional sin el que no hubiera podido llegar donde estoy.

Marta Julia López González de Quevedo
Sevilla 2021

Resumen

En el presente Trabajo Fin de Grado se realiza un estudio de sistemas que permiten la identificación de personas que acceden a un determinado recinto comercial, con el fin de realizar estadísticas de la periodicidad de las visitas y la detección de nuevos visitantes. Los distintos métodos propuestos van desde sistemas de visión artificial, pasando por la detección de identificadores únicos del teléfono móvil, o combinaciones de distintas tecnologías.

Después de valorar las ventajas e inconvenientes de cada uno de ellos, se ha realizado un prototipo de un captador pasivo de *International Mobile Subscriber Identity* (IMSI) a partir de un receptor de radiofrecuencia capacitado para trabajar en la distribución de frecuencias de la telefonía móvil.

Por último, dicho prototipo ha sido ensayado durante varios días en distintos intervalos temporales. La información recogida se ha almacenado y procesado en una base de datos, a partir de la cual se han obtenido los resultados deseados.

Abstract

In this Degree Final Project, a study of person identification systems while accessing a commercial area has been developed, in order to perform statistics on the frequency of visits and the detection of new visitors. The proposed methods range from artificial vision systems, to the detection of cell phone unique identifiers, or multiple technologies combination.

After evaluating the advantages and disadvantages of each of them, a prototype of a pasive *International Mobile Subscriber Identity* (IMSI) catcher has been made from a radiofrequency receiver capable of working in the mobile telephony frequency distribution.

Finally, the prototype has been tested for several days at different time intervals. The information collected was stored and processed in a database, from which the desired results were obtained.

Índice

Resumen III
Abstract V
Glosario IX

1 Introducción **1**
1.1 Motivación y Contexto 1
1.2 Objetivos 2

2 Métodos de identificación **3**
2.1 Estado del Arte 3
2.2 Visión Artificial 5
2.2.1 Detección basada en contornos 5
2.2.2 Histograma de Gradientes Orientados 5
2.2.3 Patrón Binario Local 6
2.2.4 Redes Neuronales Profundas 6
2.2.5 Comparación de Algoritmos 7
2.2.6 Identificación y reidentificación facial 9
2.3 Bluetooth 10
2.4 WiFi 12
2.5 IMSI 13
2.6 Síntesis y justificación de la tecnología elegida 15

3 Solución desarrollada **17**
3.1 Funcionamiento de la telefonía móvil 17
3.2 Estructura de la red de telefonía 19
3.3 Espectro radioeléctrico 21
3.4 Protocolos de red y envío de IMSI 22
3.4.1 GSM (2G) 22
3.4.2 UMTS (3G) y LTE (4G) 23
3.4.3 5G 24
3.5 Hardware y Software elegidos 25
3.5.1 Hardware 25
3.5.2 Software 26

4 Validación experimental **27**
4.1 Instalación y puesta en marcha 27
4.2 Elección de estación base 31
4.3 Captura de paquetes de la red telefónica 34
4.4 Posicionamiento de dispositivos 37
4.5 Estudio de Periodicidad 40

5 Conclusiones y desarrollo futuro **49**

Índice de Figuras 51
Índice de Tablas 52
Bibliografía 55

Glosario

AIR *Authentication Initiation Request*. 23

AKA *Authentication and Key Agreement*. 23, 24

ARFCN *Absolute Radio-Frecuency Channel Number*. 30

AuC *Authentication Center*. 22

AUTN *Authentication Token*. 23

BSC *Base Station Controller*. 19

BTS *Base Transceiver Station*. 19

CID *Cell ID*. 30, 31, 34

CK *Cipher Key*. 23

CNAF Cuadro Nacional de Atribución de Frecuencias. 21

DNN *Deep Neural Network*. 5

eNode B *Enhanced Node B*. 19

EPC *Evolved Packet Core*. 20

Faster R-CNN *Faster Region Based Convolutional Neuronal Network*. 6

GGSN *Gateway GPRS Support Node*. 20

GSM *Global System for Mobile*. 19, 21, 22, 24, 26

HLR *Home Location Register*. 22, 23

HSS *Home Subscriber System*. 23

ICCID *Integrated Circuit Card IDentifier*. 13

IK *Integrity Key*. 23

IMEI *International Mobile Equipment Identity*. 13

IMSI *International Mobile Subscriber Identity*. III, 3, 13, 22–24, 34, 35, 40, 41, 49, 50

IP *Internet Protocol*. 12, 20

KDF *Key Derivation Function*. 23

Ki *Individual subscriber authentication Key*. 22

LAC *Location Area Code*. 30, 31

LBP *Local Binary Pattern*. 6

LDR *Light Dependent Sensor*. 1

LTE *Long Term Evolution*. 17, 19, 21–23, 26

MAC *Message Autorization Code*. 23

MAC *Media Access Control*. 10, 12, 15, 49

MCC *Mobile Country Code*. 13, 30, 34

MME *Mobility Management Entity*. 20, 23

MNC *Mobile Network Code*. 13, 30, 31, 34

MS *Mobile Station*. 19

MSC *Mobile Switching Center*. 20, 22

MSISDN *Mobile Station Integrated Services Digital Network*. 13

PGW *Packet Data Network Gateway*. 20

RNC *Radio Network Controller*. 19

RSS *Received Signal Strength*. 37–39

RSSI *Received Signal Strength Indicator*. 10

SDR *Software Defined Radio*. 25, 28, 49

SGSN *Serving GPRS Support Node*. 20, 23

SGW *Serving Gateway*. 20

SIA *Subscriber Identity Authentication*. 22

SIM *Subscriber Identity Module*. 3, 22, 23

SRES *Signed Response*. 22

SSD *Single Shot Detector*. 7

SUPI *Subscriber Permanent Identifier*. 24

SVM *Support Vector Machine*. 2, 5, 6

TDT Televisión Digital Terrestre. 21

TMSI *Temporary Mobile Subscriber Identity*. 13, 34, 40, 50

UMTS *Universal Mobile Telecommunications System*. 17, 19, 21–23, 26

USIM *Universal Subscriber Identity Module*. 23

XMAC *Expected Message Authentication Code*. 23

XRES *Expected Response*. 23

YOLO *You Only Look Once*. 7

1 Introducción

1.1 Motivación y Contexto

Los sistemas de conteo tratan de estimar el número de personas en espacios, tanto exteriores como interiores. Entre la multitud de aplicaciones para esta tecnología, se destaca su utilización en superficies comerciales, donde aportan información para optimizar los horarios de apertura, además de evaluar el atractivo de ciertos artículos o campañas de ventas [1]. Por otro lado, muchos sistemas de seguridad requieren de detección y seguimiento de personas, como estimadores de colas, monitorización de entradas, aeropuertos o estaciones [2].

Desde el punto de vista del marketing, el conteo de visitas es una de las estadísticas fundamentales, referido tanto a tiendas físicas como comercio online [3]. Entre las ventajas de medir la afluencia de clientes se encuentran: conocer las preferencias de los clientes, cuánto tiempo pasan en un establecimiento y qué áreas específicas visitan; capacidad para optimizar los horarios de personal, permitiendo una mejor atención en las franjas estadísticamente más concurridas; medir y mejorar las efectividad de las campañas publicitarias así como entender los factores externos que afectan a un negocio, como el clima o festividades [4].

Más allá de las aplicaciones directas, la información dada por el sistema de conteo puede ser utilizada para calcular otras métricas que reflejan el éxito de un negocio y de las estrategias utilizadas. Destacan la Tasa de conversión, ratio entre el número de ventas y el número de visitas, y la Tasa de pérdida de suscriptores (número clientes al principio del año - número de clientes al final del año / número de clientes al principio del año) [5]. Por otra parte, existe la posibilidad no solo de conocer el número de visitas, sino de estudiar la periodicidad de acceso para cada una de ellas, suponiendo un indicador de la fidelidad del cliente.

Las primeras aproximaciones de métodos de detección se basaban en tornos giratorios o en alfombras de contacto. Dichos sensores son válidos para situaciones con poca concurrencia, ya que implican contacto e interrumpen el paso. Asimismo, otros métodos no obstructivos, como sensores *Light Dependent Sensor* (LDR) [6], ultrasonidos o térmicos, incorporan problemas a la hora de contar varias personas al mismo tiempo en situaciones de gran densidad de tráfico [7].

Como resultado del desarrollo de las tecnologías de visión por computador se idearon soluciones que resuelven los problemas de obstrucción y paso simultáneo de personas, además de conseguir mayor precisión, con sistemas más baratos y no intrusivos [8]. Haritaoglu et al. (1999) [9] propone

un sistema de conteo en tiempo real a partir de extracción del fondo y detección de siluetas, siendo capaz de identificar individuos parcialmente ocultos y realizar seguimiento mediante comparaciones de patrones. Métodos más modernos basados en visión por computador utilizan algoritmos de detección de bordes [10] o segmentación mediante umbralización (*thresholding*) y búsqueda de contornos [11]. Desde el aprendizaje automático, se incluyen soluciones de detección facial basadas en *Support Vector Machine* (SVM), un método de aprendizaje supervisado para resolver métodos de clasificación [1].

En este contexto de potencial económico y antecedentes teóricos, se propone investigar las diferentes posibilidades de desarrollo de un sistema de conteo, con el fin de encontrar una alternativa económica, precisa y que permita la reidentificación de un mismo individuo en futuros accesos o la incorporación de un nuevo cliente, es decir, estudiar a su vez la periodicidad.

1.2 Objetivos

El objetivo general de este Trabajo Técnico es analizar y comparar distintos sistemas que permitan la identificación única de personas en su acceso a un recinto específico. Dentro del objetivo general se incluye el desarrollo de un prototipo del sistema que se considere más prometedor.

Este objetivo general requiere el cumplimiento de los siguientes subobjetivos, que se abordan en el trabajo:

1. Identificar las potenciales soluciones al problema de conteo, teniendo en cuenta sus aplicaciones reales, ventajas y desventajas y realizando un estudio económico en el caso de su implementación.

2. Justificar la tecnología elegida como más prometedora y realizar un estudio a fondo sobre su implementación. Buscar opciones software y hardware para su desarrollo.

3. Desarrollar un prototipo a partir de los sistemas elegidos. Realizar ensayos y analizar los resultados obtenidos con ayuda de una base de datos.

4. En base a los resultados, determinar la escalabilidad a una aplicación real, además de posibles mejoras y lineas de investigación futuras.

2 Métodos de identificación

Al comienzo de este capítulo se reflejan diferentes soluciones ya implementadas que componen el estado del arte del proyecto. A continuación, se realiza un estudio de las aplicaciones y la viabilidad de las siguientes tecnologías para diseñar un sistema de conteo con posibilidad de reidentificación y estudio de la periodicidad de acceso. Las tecnologías propuestas son: Visión Artificial, Bluetooth, WiFi e identificador IMSI de la tarjeta *Subscriber Identity Module* (SIM). Por último, se realizará una síntesis de las ventajas y desventajas de los sistemas descritos, justificando la elección a partir de la cual se desarrollará el prototipo.

2.1 Estado del Arte

A la hora de desarrollar una aplicación real, es importante revisar el estado del arte de la tecnología, con el fin de crear un sistema actualizado y que cumpla con las especificaciones impuestas por sus predecesores.

En el momento actual existen numerosas opciones comerciales de sistemas de conteo y seguimiento de personas, muchas de ellas basadas en las tecnologías propuestas en este trabajo.

Un ejemplo de esto es el servicio *SmartCounter* ofrecido por la empresa española *Proconsi*. Se trata de un sistema de conteo de aforo en tiempo real que, utilizando Visión Artificial, controla las entradas y salidas de un recinto. Además, ofrece la incorporación de cámaras termográficas para controlar así la temperatura de los asistentes [12]. En la misma línea también se encuentra el servicio *iSolutions* con un modelo de cámaras situadas de igual manera en entradas y salidas, que a su vez pueden tener aplicaciones de seguridad [13].

Otra opción disponible en el mercado es la propuesta por *Verticales Retail*. A través una red *WiFi* disponible para los clientes, es posible estudiar la afluencia, tiempo de estancia, fidelización, así como generar métricas esenciales para un negocio. Asimismo, ofrece una conexión a internet segura y posibilita una mejor comunicación a través de una aplicación móvil [14].

Por otro lado, otras soluciones como *Insight* de *Flame Analytics* o *FEVOX* integran varias de estas opciones. Ambos sistemas combinan el conteo por vídeo junto al seguimiento a través de *WiFi*. La unión de ambas tecnologías permite disponer de un conteo preciso de entradas y salidas junto a la posibilidad de realizar un análisis de presencia de los clientes, calculando ratios de conversión, tiempos de estancia y fidelidad [15, 16].

La Figura 2.1 muestra un ejemplo de interfaz de análisis de datos, donde el número de visitas, tiempo medio de estancia o intervalos de mayor concurrencia son representados gráficamente facilitando su interpretación.

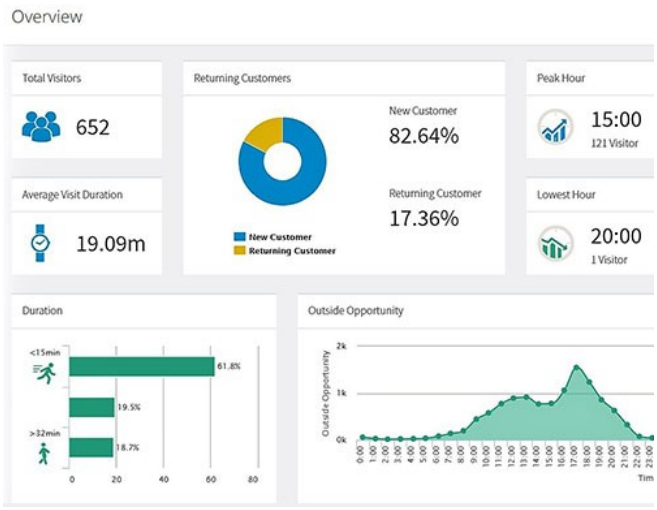

Figura 2.1 Plataforma de Análisis de información y generación de reportes [16].

Por último, mencionar *Lifeseeker*, un sistema aéreo de localización de teléfonos móviles. Está diseñado para facilitar las misiones de rescate de los servicios de emergencia, siendo capaz de ubicar de forma precisa un dispositivo sin la colaboración de la persona, en zonas con y sin cobertura. Actualmente, está disponible en varios modelos para helicópteros, aeronaves y drones, siendo capaz de operar en condiciones atmosféricas extremas [17].

2.2 Visión Artificial

El creciente desarrollo de la visión por computador y el análisis de imagen y vídeo, hacen que las alternativas de desarrollo de un sistema de conteo sean muy variadas. Por otro lado, el uso extendido de cámaras de vigilancia tanto en interiores como en exteriores, implica más facilidades de implementación de este tipo de sistemas.

Uno de los principales retos de las propuestas basadas en imágenes es la detección precisa de personas en distintos escenarios, ya sea por el continuo movimiento de la multitud en varias direcciones, cambios en la iluminación o en el fondo de la imagen. Si la detección es correcta, el conteo es sencillo, por tanto, nos centraremos en estudiar y comparar los algoritmos más utilizados para detección de personas [18]. Los métodos elegidos son: Detección basada en contornos, Histograma de Gradientes Orientados, Patrón Binario Local y Redes Neuronales Profundas (*Deep Neural Network* (DNN)).

2.2.1 Detección basada en contornos

Se trata de un método fácil y sencillo de implementar. Puesto que las personas en un vídeo nunca estarán estáticas, siempre habrá un mínimo cambio, se utiliza la información del movimiento como criterio para el algoritmo. Para cada fotograma, se diferencia entre fondo (objetos estáticos) y primer plano (objetos en movimiento). Al primer plano se le aplica dilatación, operación morfológica utilizada en procesamiento de imagen para rellenar huecos. Se buscan los contornos de los objetos en movimiento sobre la imagen dilatada, se estima el área de cada objeto y se filtra en torno a un rango de área para eliminar falsos positivos. Los objetos en el rango definido son identificados como personas [19]. Este algoritmo presenta inconvenientes en caso de solapamientos, además de la aparición de falsos positivos si hay objetos inanimados en movimiento que se encuentren dentro del rango especificado.

2.2.2 Histograma de Gradientes Orientados

Es una técnica de detección de objetos que utiliza la distribución de gradientes de intensidad, es decir, detección de bordes como descriptor de características. El gradiente de una imagen mide como cambia esta en términos de color o de intensidad. La magnitud del vector gradiente indica la rapidez del cambio, mientras que la orientación indica la dirección hacia la que cambia.

Un descriptor de características tiene como objetivo generalizar un objeto, de forma que el mismo objeto produzca un descriptor de características muy similar cuando se observa en distintas condiciones. El método estudiado descompone la imagen en celdas y calcula los gradientes para cada una de ellas. El histograma combinado de todas las celdas representa el descriptor. Una vez detectadas las características de las imágenes, la detección de personas se convierte en un problema de clasificación, para el que se suele utiliza comúnmente una máquina de vector soporte (SVM) [18].

Una SVM es una técnica de *Machine Learning* que encuentra la mejor separación posible entre clases. En un problema de clasificación de dos dimensiones, la separación es una línea, pero los problemas comunes tienen muchas dimensiones, por lo que la SVM encuentra el hiperplano que maximiza el margen de separación entre clases. Los vectores de soporte son los puntos que definen el margen de separación del hiperplano que separa las clases [20].

La Figura 2.2 muestra el problema de clasificación en 2D. Suponiendo que los puntos azules corresponden a la clase azul y los puntos rojos a la clase rojo, se hayan los vectores de soporte que maximiza la distancia entre ambas clases.

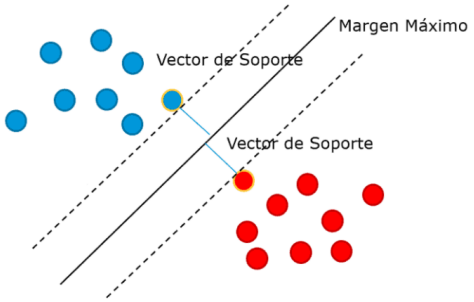

Figura 2.2 Vector de Soporte en 2D [20].

Para la detección de personas se toman dos conjuntos de datos, uno que contiene personas y otro que no. A partir de muestras de ambos conjuntos, a las que se les calcula el histograma de gradientes, se entrena la SVM, haciéndola capaz de localizar personas en imágenes. Para cada fotograma, se extraen los gradientes y se pasan al clasificador preentrenado, que devuelve la posición de las posibles personas de la imagen.

2.2.3 Patrón Binario Local

El *Local Binary Pattern* (LBP) es un descriptor de texturas simple y efectivo. Para cada píxel de la imagen, se examinan sus 8 píxeles vecinos y se compara cada uno con el central. Si el vecino es mayor que el central, se etiqueta como 1 y si es menor como 0. Con estos valores, se codifica una cadena binaria de 8 bits para cada píxel de la imagen, similar al histograma de una muestra en escala de grises [21].

Al igual que ocurre con el histograma de gradientes orientados, es necesario utilizar un clasificador para detectar y posicionar las características extraidas. Para este caso, el algoritmo clasificador utilizado es *AdaBoost*, contracción de *Adaptative Boosting*, un método utilizado en *Machine Learning* basado en árboles de decisión. La técnica *boosting* consiste en crear clasificadores robustos a partir de la adición de clasificadores débiles, variando el peso que tiene cada uno de ellos [22].

El procedimiento a seguir es similar al descrito anteriormente: se toman dos conjuntos, uno conteniendo personas y otro no. Se toman muestras de ambos, asegurando que el número de imágenes que no presentan personas es mucho mayor que el que sí las contienen. Para cada imagen se extraen sus características según el patrón binario local. Además, para las muestras que incluyen personas, se anota el número de sujetos y las coordenadas x e y en las que se encuentran. Con esta información se entrena el modelo clasificador, por el que pasarán los rasgos extraídos para cada uno de los fotogramas del vídeo, con el fin de detectar a los transeúntes.

2.2.4 Redes Neuronales Profundas

Las opciones de solución basadas en aprendizaje profundo (*Deep Learning*) para problemas de detección son variadas e incluyen *Faster Region Based Convolutional Neuronal Network* (Faster

R-CNN), *You Only Look Once* (YOLO) y *Single Shot Detector* (SSD). A la hora de compararlos, hay que tener en cuenta su precisión y tiempo de computación. El procesamiento del algoritmo YOLO es mucho más rápido que una R-CNN, a costa de perder precisión. Los SSD, son intermedios entre estos dos métodos.

La solución propuesta por Padmashini et al. (2018) [19], combina la arquitectura MobileNets [23] con SSD, obteniendo una detección más rápida eficiente. Una vez el modelo *MobileNetSSD* es entrenado, se le pasa como entrada cada uno de los fotogramas del vídeo deseado, obteniendo como salida las coordenadas de las personas detectadas.

2.2.5 Comparación de Algoritmos

Para evaluar y comparar correctamente los algoritmos estudiados es esencial elegir las métricas correctas. A continuación se definen unos términos muy utilizados en *Machine Learning*, que ayudan a describir el comportamiento del modelo y a calcular dichas métricas.

Se definen como Verdaderos Positivos (VP), aquellas personas que son correctamente clasificadas como tal por el algoritmo. En el caso de las personas que no son detectadas, se habla de Falsos Negativos (FN). Se habla de Falso Positivo (FP) cuando un objeto es erróneamente clasificado como humano. Por último, los Verdaderos Negativos (VN) serían objetos correctamente clasificados como no humanos. En el caso de detección de personas, esta medida no se considera ya que el algoritmo no está entrenado para identificar objetos.

Conociendo estos términos, se procede a definir las métricas con las que se compararán las técnicas descritas anteriormente.

- *Accuracy* (Exactitud): estima como de correcto es el algoritmo. Es la proporción de predicciones correctas entre todas las predicciones hechas.

$$Accuracy = \frac{VerdaderosPositivos + VerdaderosNegativos}{VP + VN + FP + FN} \tag{2.1}$$

- *Precision* (Precisión): mide la proporción de personas correctamente identificadas como tal, entre todas las personas detectadas.

$$Precision = \frac{VerdaderosPositivos}{VerdaderosPositivos + FalsosPositivos} \tag{2.2}$$

- *Recall* (Exhaustividad): mide cuantos individuos es capaz de detectar el modelo en proporción al número real de personas en la imagen.

$$Recall = \frac{VerdaderosPositivos}{VerdaderosPositivos + FalsosNegativos} \tag{2.3}$$

- *F-Score* (Valor-F): combina las medidas de *precision* y *recall* a partir de la media armónica de ambos valores

$$F - Score = \frac{2 * Precision * Recall}{Precision + Recall} \tag{2.4}$$

- *Precision* (Precisión): mide la proporción de personas correctamente identificadas como tal, entre todas las personas detectadas.

$$Precision = \frac{VerdaderosPositivos}{VerdaderosPositivos + FalsosPositivos} \tag{2.5}$$

Se evalúan los algoritmos propuestos a partir de los experimentos realizados por Padmashini et al. [19]. La Tabla 2.1 muestra las medidas recogidas en dichos experimentos.

Tabla 2.1 Comparación de Medidas. Total de personas: 6074.

ALGORITMO	MEDIDAS			
	VP	FP	FN	VP
Contornos	2926	1411	3148	0
Patrón Binario Local	3289	1345	2785	0
Histograma Gradientes Orientados	2771	30	3303	0
Redes Neuronales	5632	121	442	0

Evaluando las métricas anteriormente descritas en función de los datos se obtienen los resultados que se muestran en la Tabla 2.2.

Tabla 2.2 Evaluación de las métricas para cada algoritmo.

ALGORITMO	MÉTRICAS			
	Accuracy	Precision	Recall	F-Score
Contornos	0.4076	0.6118	0.5255	0.5206
Patrón Binario Local	0.4831	0.7353	0.6048	0.6197
Histograma Gradientes Orientados	0.5046	0.9807	0.5120	0.6389
Redes Neuronales	0.9053	0.9855	0.9152	0.9393

Se observa que el algoritmo basado en contornos es el peor de los comparados, ya que no es capaz de detectar dos personas muy cercanas entre sí sin superponerlas. Es interesante también el número tan bajo de falsos positivos con el Histograma de Gradientes Orientados, a pesar de que el número de Verdaderos Positivos también es menor en comparación con el resto de modelos.

El comportamiento del modelo basado en redes neuronales es, con diferencia, mejor que los otros algoritmos estudiados, cumpliendo con la exactitud y precisión requeridas para este tipo de sistemas.

No obstante, los modelos propuestos permiten la detección, más o menos precisa, de personas, pero no la reidentificación. La reidentificación de personas trata de determinar si la imagen de un individuo en distintas cámaras, o distintas condiciones, pertenece a la misma persona. A corto plazo, características como la ropa o la apariencia física facilitan el problema, sin embargo, es más interesante estudiarlo a largo plazo, por la posibilidad de conocer la frecuencia de acceso de visitantes a un recinto. Con este objetivo, una de las principales líneas de investigación se centra en el reconocimiento facial.

2.2.6 Identificación y reidentificación facial

Entre las medidas biométricas visuales utilizables para identificar a una persona a través de imágenes, como la forma del cuerpo, ropa, iris o forma de caminar, los rasgos faciales se consideran entre los más fiables, ya que son más estables respecto a cambios espaciales y temporales. Otros rasgos, como las huellas dactilares, pueden ser invariables en el tiempo, pero también son más invasivos.

Uno de los principales problemas de la reidentificación reside en la falta de imágenes de alta calidad para extraer características y entrenar modelos, ya que la fuente de datos son cámaras de seguridad. Los modelos entrenados con conjuntos de datos de caras en alta resolución no dan buenos resultados al implementarlos con imágenes de seguridad reales.

Estudios recientes [24, 25, 26] exponen que los modelos existentes no son lo suficientemente buenos para conseguir reidentificación a partir de imágenes de baja resolución. No obstante, con el rápido avance de las redes neuronales, se prevé que en un futuro cercano la reidentificación facial a gran escala sea un problema asequible.

2.3 Bluetooth

La tecnología Bluetooth lleva usándose como método de posicionamiento y seguimiento desde su implementación generalizada en los teléfonos móviles. La metodología para el *tracking* se basa en instalar escáneres que buscan las señales emitidas por los dispositivos y registran cada detección, a partir de la cual se aproxima la distancia al escáner.

El Bluetooth facilita el conteo y seguimiento sin necesidad de participación ni esfuerzo por parte de los clientes. La identificación individual, y por lo tanto el conteo, es posible por la transmisión de la dirección *Media Access Control* (MAC), identificador único de cada dispositivo. Este, además de la posibilidad de ver la trayectoria seguida a lo largo del local, permite comprobar la periodicidad de acceso, en el caso de que la dirección MAC se repita en distintos días.

En un dispositivo, existen tres posibles estados de la señal Bluetooth: apagado, encendido y visible o encendido e invisible. Un receptor solo será capaz de detectar aquellos que tengan la señal encendida y visible, limitando el número de personas captadas. Por otro lado, existe el caso en el que un mismo individuo disponga de dos módulos con señal visible y fuera contado como dos personas diferentes. Sería posible depurar la detección si se dan trayectorias idénticas de dos identificadores a lo largo del tiempo.

Es importante tener en cuenta el rango de los receptores, así como las fuentes de interferencias que pueden afectar a las medidas: objetos físicos, radiofrecuencias, sistemas electrónicos, paredes o estructuras metálicas, que modifican de manera diferente la señal recibida.

La localización podría aproximarse a partir de la posición del escáner Bluetooth, aproximación conocida como *principio de proximidad* [27]. Una solución más compleja utiliza valores de *Received Signal Strength Indicator* (RSSI) (Indicador de la Fuerza de la Señal Recibida), como la aplicación de Oosterlinck et al. (2017) [28] sobre localización de clientes en un centro comercial. Estos valores son inversamente proporcionales a la distancia al receptor y es posible calcular una posición razonablemente precisa utilizando técnicas de triangulación a partir de las medidas de distintos escáneres.

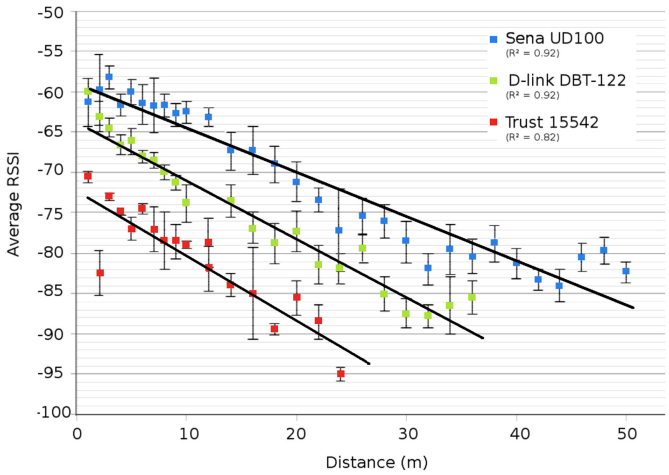

Figura 2.3 Relación RSSI y Distancia (m) para 3 modelos de receptores diferentes [28].

La Figura 2.3 muestra la relación entre la potencia de señal recibida y la distancia al emisor para

tres modelos comerciales de receptores Bluetooth. A partir de esta información es posible elegir el modelo más adecuado para cada aplicación, así como estimar la precisión de las medidas obtenidas.

En el prototipo del centro comercial, se analizan el número de clientes, las tiendas más visitadas, el nivel de fidelización de los clientes, diferencias en la distribución de visitas los días laborables y fines de semana y las duraciones medias de las visitas, entre otras métricas.

En definitiva, el conteo y *tracking* con Bluetooth proporciona mucha información, sin necesidad de interacción del público, con bajo coste y con las ventajas de privacidad que ofrecen las direcciones MAC, al no poder ser directamente asociadas a la identidad de la persona. Sin embargo, presenta limitaciones que es necesario tener en cuenta.

En primer lugar, el radio de detección es limitado, alcanzando como máximo 100 metros. Dado que para un correcto seguimiento es necesario que varios escáneres reciban señales del dispositivo, cuanto mayor sea el área a estudiar, hará falta un número mayor de receptores, aumentando a su vez el precio.

Por otro lado y como desventaja fundamental para un conteo preciso, está el hecho de que los dispositivos deban estar en modo visible para su identificación. Oosterlinck et al. (2017) [28] mide que el ratio de detección obtenido es del 9.81 % del total de visitantes. Para algunos propósitos puede ser una muestra adecuada, pero para el problema de conteo es claramente insuficiente. El hecho de que exista un modo invisible, reduce esta tasa. Es posible pedir a los clientes la activación visible de la señal Bluetooth de sus dispositivos, pero con esta acción se compromete la no interacción de la tecnología.

2.4 WiFi

El conteo y seguimiento mediante el uso de WiFi es muy similar al uso de receptores Bluetooth. Ambos utilizan la dirección MAC, única de cada dispositivo como identificador de personas.

Al igual que con Bluetooth, las direcciones MAC pueden ser detectadas con escáneres a partir de las señales que emiten los dispositivos móviles y medir la potencia de la señal recibida. No obstante, las señales WiFi están pensadas para conexiones de mayor rango que las Bluetooth, lo que las hace menos precisas a la hora de medir la distancia entre emisor y escáner.

Otra similitud se encuentra en la necesidad de tener la conexión WiFi habilitada, restringiendo el porcentaje de visitantes. Existe la posibilidad de que las personas sean menos dadas a habilitar dicha conexión fuera de sus casas. Sin embargo, Abedi et al. [29] obtienen mayor ratio de detección con WiFi que con Bluetooth, aunque lo consiguen en un recinto universitario, que provee de redes libres a las que conectarse.

En contraste con lo anterior, una opción existente con la tecnología WiFi que no ofrece Bluetooth es que el local interesado en el conteo facilite a sus clientes conexión a internet a través de una red propia. Así, el dueño de la red puede ver las direcciones MAC e *Internet Protocol* (IP) de los dispositivos conectados a ella y puede fomentar su uso ofreciendo internet seguro y de calidad.

Por consiguiente, nos encontramos con las mismas desventajas que con la anterior tecnología. No se puede esperar una medida precisa de conteo ya que la población objetivo solo es un pequeño porcentaje de los visitantes reales. A pesar de ello, el ratio de detección es suficiente para aportar métricas interesantes, en especial en los lugares que ya ofrezcan una conexión a los visitantes y no sea necesaria ninguna inversión para ponerlo en marcha.

2.5 IMSI

Con la evolución de la telefonía móvil, especialmente en la última década, no es extraño suponer que la mayoría de personas lleve consigo un móvil en todo momento. Este hecho promueve el uso de dichos dispositivos para detectar a sus propietarios, como se da en el caso de las tecnologías Bluetooth y WiFi a partir de la dirección MAC.

Existen otros identificadores que pueden resultar útiles para el problema de detección y conteo de personas.

- *Integrated Circuit Card IDentifier* (ICCID) o Identificador del Circuito Integrado de la Tarjeta. Se trata de un número de 19 cifras, único para cada tarjeta SIM, que se encuentra grabado en la superficie de ella. Pese a ser interesante por ser un identificador único, no es rastreable mediante métodos no invasivos.

- *International Mobile Subscriber Identity* IMSI o Identificador Internacional de Abonado Móvil. Es el número que identifica a un cliente y el que se utiliza para realizar las conexiones a la red. Tiene un máximo de 15 cifras, de las cuales las tres primeras indican el código del país al que pertenece (*Mobile Country Code* (MCC)), seguidas de las que señalan el operador (*Mobile Network Code* (MNC)) con longitud de dos o tres dígitos. Los números restantes identifican al cliente. El IMSI es fijo mientras el cliente permanezca con la misma operadora. Su principal ventaja es que es transmitido cada vez que el teléfono se conecta a una estación base, y esa conexión es rastreable.

- *Mobile Station Integrated Services Digital Network* (MSISDN), comunmente conocido como número de móvil. Es el que identifica a la persona, no al operador. Sin embargo, no es rastreable por métodos legales.

- *International Mobile Equipment Identity* (IMEI) o Identificador Internacional del Equipo Móvil. Se trata del identificador propio del dispositivo móvil, no tiene relación con la persona ni con la operadora. Es rastreable, pero cambiará al cambiar el dispositivo.

Con este breve repaso de los identificadores asociados a los teléfonos móviles, es ostensible que el más indicado para usar como detector es el IMSI. Su principal ventaja respecto al resto es que es interceptable.

Cada operadora dispone de una red de estaciones base distribuidas por toda la superficie de su dominio, con el fin de dar cobertura a todos sus clientes. Cuando un teléfono se mueve, está constantemente buscando la estación base que le da mayor potencia de señal en ese momento. Para realizar la conexión, el dispositivo tiene que identificarse a través de su IMSI y tras autorizarlo, móvil y estación se comunican a través de un número temporal aleatorio: *Temporary Mobile Subscriber Identity* (TMSI), para proteger la privacidad del cliente [30].

Este protocolo de comunicación ha sido aprovechado para desarrollar los llamados *IMSI catchers* o captadores IMSI. Se trata de un equipo que se hace pasar por una estación base y obliga a los dispositivos de alrededor a conectarse a ella ofreciendo mayor potencia de señal que las estaciones cercanas.

Así intercepta no solo los IMSI, sino también las comunicaciones, o incluso consiguiendo la localización. Este tipo de interceptación se denomina *Man in the middle* (hombre en medio), ya que

hace pasar las comunicaciones a través de su estación base falsa, mientras la que da soporte es una estación real. En la Figura 2.4 se representa el esquema de funcionamiento de un *IMSI catchers* activo.

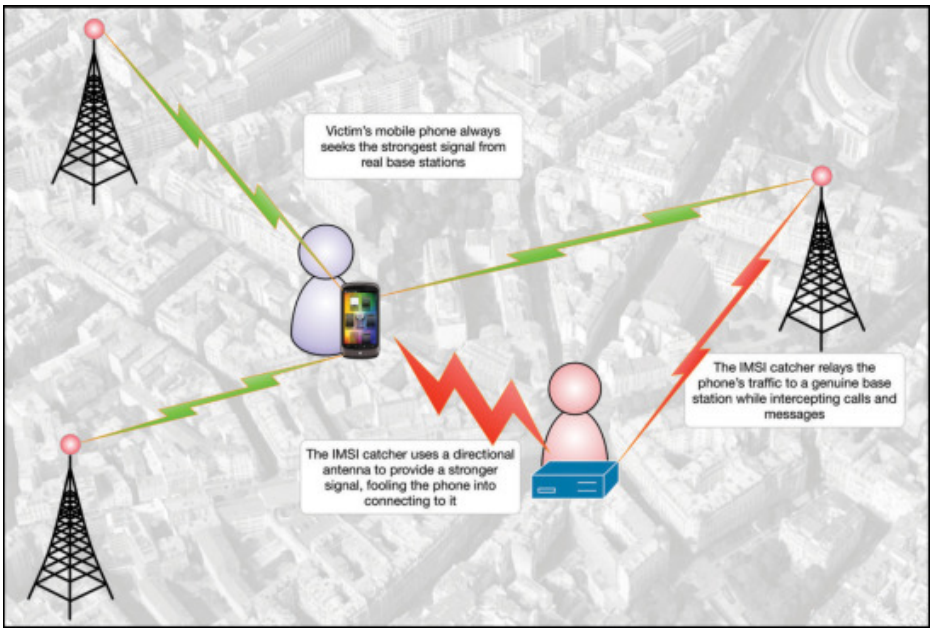

Figura 2.4 Funcionamiento *IMSI-Catcher Activo* [31].

Ha sido un método utilizado por la policía para escuchar y localizar personas en busca y captura, pero también por *hackers* para atacar y robar datos y al ser totalmente intrusivo es ilegal [32].

La alternativa legal propuesta para esta tecnología se trata de un *sniffer* o un receptor de paquetes que busca en las frecuencias asignadas a las comunicaciones móviles a que se produzca el primer intercambio entre teléfono y estación base, en el que se transmite el IMSI.

En definitiva, se eligen las estaciones base que dan cobertura a la zona deseada y se reciben las señales que llegan a las frecuencias de dichas estaciones base, entre los que se encuentran los identificadores IMSI de las personas que acceden.

Al ser único y estático, permite contar todas las visitas y además tener datos sobre la periodicidad de acceso, sin necesidad de tener activa la comunicación, como ocurre con Bluetooth y WiFi.

Entre las desventajas de esta tecnología se encuentra la posibilidad de tener sobreconteo, en el caso de que las estaciones cubran un área superior a la deseada. No obstante, es posible filtrar los datos obtenidos en función de la potencia de la señal recibida o de la banda en la que se ha detectado.

2.6 Síntesis y justificación de la tecnología elegida

Finalmente, tras estudiar las posibles soluciones del problema, se procede a comparar su viabilidad con el objetivo de elegir aquella sobre la que se desarrollará un prototipo que se describe en los siguientes capítulos.

En primer lugar, los modelos de Visión Artificial, en especial el basado en redes neuronales profundas, dan muy buenos resultados a la hora del conteo de personas. Sin embargo, respecto a la reidentificación de personas, los modelos actuales no son lo suficientemente buenos para llevarla a cabo con imágenes de baja resolución y sobre un conjunto de personas desconocido.

Por otro lado, el uso de detectores Bluetooth presenta la ventaja de poder seguir el recorrido de los clientes a lo largo del local, usando varios escáneres de bajo coste y aplicando algoritmos de triangulación. Además, el uso de la dirección MAC permite la reidentificación en futuras visitas y el anonimato del cliente al no estar directamente relacionado con su persona. Su principal desventaja reside en la necesidad de tener la señal Bluetooth activada y visible para ser detectada. Así, disminuye el ratio de dispositivos identificados respecto al número total de visitas, requiriendo también la cooperación del cliente.

De forma análoga a la tecnología Bluetooth, las redes WiFi permiten la detección y localización de individuos a partir de las direcciones MAC de los dispositivos dentro de su rango de acción. Existe también la opción de instalar una red WiFi a la que los clientes puedan acceder libremente para obtener conexión a internet y recoger las direcciones y el tiempo de conexión de los dispositivos que la utilicen. Comparte también la necesidad de tener la señal WiFi activada para que el dispositivo sea detectable, disminuyendo el ratio de detección.

Por último, el uso del número IMSI para identificar dispositivos únicos no requiere la activación de ninguna señal, ni presenta problema a la hora de estudiar la periodicidad de acceso. Además, el receptor que se utiliza para leer las frecuencias de telefonía no tiene un gran coste. Los inconvenientes que puede presentar se deben a que la localización y rango de las estaciones base son competencia de las operadoras de telefonía, pudiendo cubrir más área de la deseada y llevando a un sobreconteo.

Tabla 2.3 Resumen Métodos de Identificación y Conteo.

TECNOLOGÍA	VENTAJAS	DESVENTAJAS
Visión Artificial	• Método de conteo preciso	• No detecta personas únicas ni da datos de frecuencia de acceso • Los modelos de reidentificación no están lo suficientemente avanzados
Bluetooth	• Seguimiento dentro del local • Posibilidad de reidentificación • Bajo coste	• Limitación del ratio de detección a los dispositivos con Bluetooth activo en modo visible
WiFi	• Posibilidad de reidentificación • Bajo coste o nulo (si ya cuenta con red WiFi)	• Limitación del ratio de detección a los dispositivos con WiFi activo
IMSI	• Posibilidad de reidentificación • Bajo coste • Detecta todos los dispositivos en el área	• Posibilidad de sobreconteo

La Tabla 2.3 recoge las principales características a favor y en contra de cada una de las tecnologías anteriormente mencionadas.

Considerando las opciones estudiadas y dando importancia tanto al conteo como al estudio de la frecuencia de acceso, el prototipo propuesto, desarrollado en el presente TFG, es un receptor de IMSI. En el siguiente capítulo se detalla el hardware y software elegido, así como la base teórica en la que se fundamenta.

3 Solución desarrollada

En este capítulo se desarrolla la base teórica del prototipo a diseñar, entre la que se encuentra el funcionamiento y estructura de las comunicaciones móviles, identificación de dispositivos y cifrado de mensajes. Además se describen el Hardware y Software elegidos y las pruebas que se realizarán con ellos.

3.1 Funcionamiento de la telefonía móvil

En el momento actual, la telefonía móvil e Internet son las dos tecnologías de comunicación más importantes y evolucionan a un ritmo imparable. En los últimos años se ha desarrollado la tecnología 5G, que a su vez convive con los sistemas 4G (*Long Term Evolution* (LTE)) y 3G (*Universal Mobile Telecommunications System* (UMTS)).

La telefonía se basa en el concepto de "celular", que hace posible la reutilización de frecuencias, que son muy limitadas, dar acceso a un gran número de usuarios y crear un sistema más eficiente. Los sistemas celulares tratan de utilizar estaciones base de pequeña y mediana potencia dando acceso a un área más reducida. La zona de cobertura a la que abastece una estación base se conoce como "célula". En cada célula solo se puede utilizar un conjunto de frecuencias dentro del total que la operadora tenga asignada y es necesario utilizar muchas células para cubrir todo el territorio.

Si dos células comparten las mismas frecuencias se puede producir la llamada interferencia cocanal, es decir, si una señal a determinada frecuencia es interferida por otra señal de la misma frecuencia con potencia similar o mayor, es imposible demodularla.

La ventaja de los sistemas celulares se encuentra en que si las células están alejadas entre sí pueden reutilizar el mismo rango de frecuencias sin interferir entre ellas.

Un sistema celular se forma dividiendo el territorio al que se le da cobertura en celdas o células, principalmente hexagonales, cada una de las cuales tiene una estación base que le da cobertura utilizando una cierto rango de frecuencias. El espectro de frecuencias puede ser reutilizado, siempre que se eviten las interferencias entre células próximas.

Cuanto menores sean las células, más canales soportará el sistema, al poder asignar conjuntos de frecuencias diferentes para células diferentes. Cuando se realiza la planificación, se comienza con células muy grandes y se va disminuyendo su tamaño conforme aumenta el número de usuarios.

Si en una celda hay más tráfico del permitido, se puede dividir añadiendo más estaciones base y disminuyendo la potencia de transmisión. Es lo que ocurre en zonas urbanas, donde la distancia entre estaciones base es del orden de cientos de metros.

A la hora de dividir el terreno en células se utilizan formas hexagonales, ya que para un radio fijo, el hexágono es el polígono regular que ocupa más superficie. La utilización de formas circulares se descarta por la superposición que se produciría en los límites entre dos células, resultando un modelo poco eficiente. A cada una de las divisiones hexagonales se las llama sectores. Las estaciones base se suelen ubicar en la unión de tres sectores, utilizando antenas con un diagrama de radiación horizontal separadas 120º entre sí, como se observa en la Figura 3.1 [33].

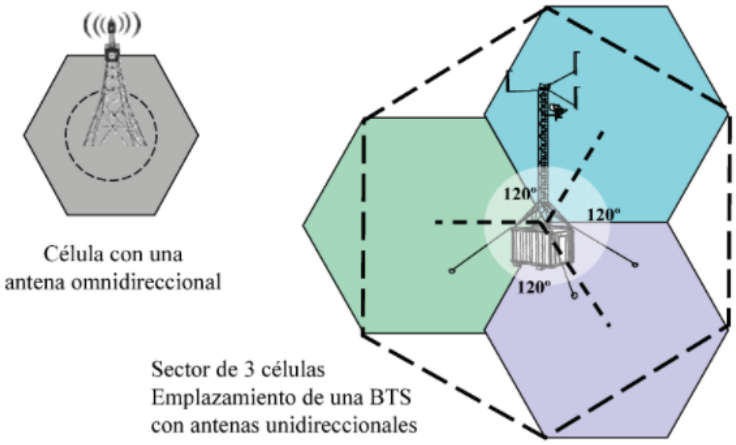

Figura 3.1 Emplazamiento estaciones base [33].

3.2 Estructura de la red de telefonía

En el momento actual conviven tres generaciones de redes de telefonía móvil: 2G, 3G y 4G, estando en proceso de implementación una cuarta (5G). Cada una de ellas tiene elementos diferentes, pero existen elementos comunes para permitir el paso de los usuarios de una a otra. La Figura 3.2 muestra los elementos principales de la red para las distintas generaciones.

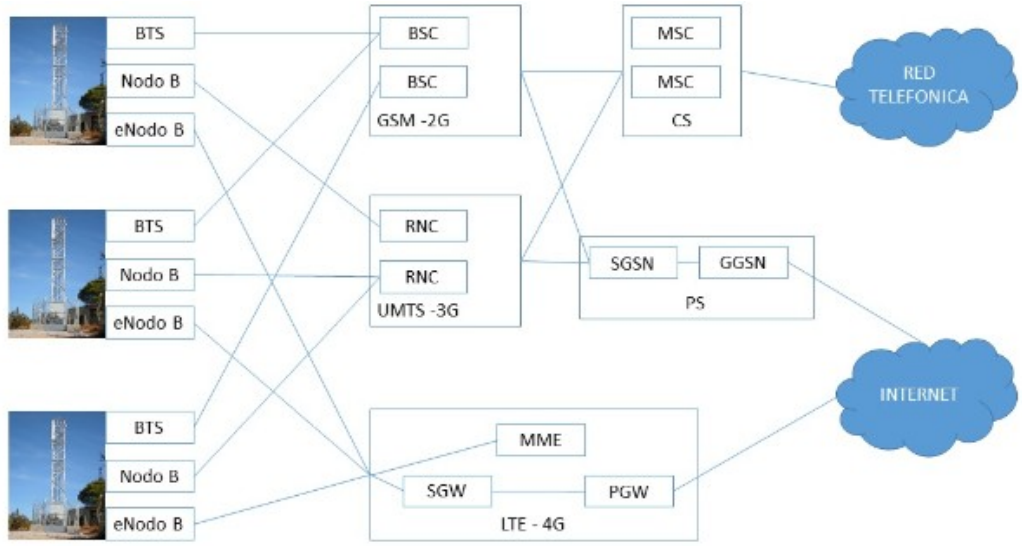

Figura 3.2 Arquitectura de las redes GSM, UMTS y LTE [34].

Estaciones Móviles

Las *Mobile Station* (MS) suministran servicio a los usuarios en cualquier lugar e instante. Existe una gran variedad de dispositivos, y los más comunes son los *smartphones* y *tablets*. Pueden actuar como emisores o receptores y se comunican con las estaciones base para tener acceso a la red [33].

Estaciones Base

Denominadas *Base Transceiver Station* (BTS) para la red *Global System for Mobile* (GSM) (2G), Nodo B para UMTS (3G) y *Enhanced Node B* (eNode B) para LTE (4G). Se encargan de mantener el enlace entre las estaciones móviles y las estaciones de control [33].

Estaciones de Control

Base Station Controller (BSC) para GSM y *Radio Network Controller* (RNC) para UMTS. En el caso de 4G, los eNode B incorporan tanto las funciones de las estaciones base como las de control. Realizan las funciones de gestión y mantenimiento de la red. Entre sus tareas se encuentra la asignación de estaciones base a las estaciones móviles de la zona. Existe una función de conmutación entre estaciones base, que permite cambiar el canal ocupado por una estación móvil por otro libre en la estación base más cercana [33].

Elementos de conexión a la red telefónica

Las *Mobile Switching Center* (MSC) o centros de conmutación son las centrales que establecen las llamadas de voz en redes móviles y fijas. A este elemento se conectan tanto las BSC como las RNC, para dar acceso a llamadas de voz a 2G y 3G.

Elementos de conexión a internet

Para la conexión a internet, la segunda y la tercera generación siguen un camino diferente a la cuarta [34].

- **GSM y UMTS**: Las BSCs y RNCs envían los datos al *Serving GPRS Support Node* (SGSN), que tiene como función dar acceso a los terminales móviles hacia la red de datos. De ahí pasa al *Gateway GPRS Support Node* (GGSN), elemento final en la conexión.
- **LTE**: en 4G la conexión se realiza a través del *Evolved Packet Core* (EPC), compuesto por
  - *Mobility Management Entity* (MME): nodo principal de control, gestiona la red y realiza la identificación del usuario.
  - *Serving Gateway* (SGW): recibe las comunicaciones de los eNodes B y se encarga de gestionar los cambios de los dispositivos móviles entre un nodo y otro.
  - *Packet Data Network Gateway* (PGW): sustituye al GGSN como frontera entre la red móvil y la red externa de operador. Asigna las direcciones IP de cada usuario.

3.3 Espectro radioeléctrico

De lo expuesto anteriormente se concluye que las frecuencias disponibles son limitadas. Según el Ministerio de Asuntos Económicos y Transformación Digital [35], se define el Espectro Radioeléctrico como "un bien de dominio público cuya titularidad y administración corresponden al Estado". En sí, es el medio físico por el cual se transmiten las ondas electromagnéticas y está administrado por cada país.

Está compuesto por un conjunto de frecuencias, conocidas como "bandas de frecuencias" comprendidas entre 8.3 kHz y 3000 GHz, cuya distribución está especificada en el Cuadro Nacional de Atribución de Frecuencias (CNAF) publicado en el Boletín Oficial del Estado [36]. Mediante subastas, el gobierno concede el uso de bloques de frecuencias.

Dentro del espectro, se encuentran las bandas de frecuencia asignadas a la telefonía móvil, definiéndose un mapa de frecuencias en función de las generaciones y las operadoras. Las bandas asignadas en España son las siguientes:

- Banda 700 MHz. Utilizada por la Televisión Digital Terrestre (TDT), utilizada para la implementación de 5G.
- Banda 800 MHz o banda 20. Utilizada por la TDT y liberada para la implantación del LTE (4G).
- Banda 900 MHz o banda 8. Utilizada primero por GSM (2G) y actualmente por UMTS (3G).
- Banda 1800 MHz o banda 3. Inicialmente asignada para 2G, actualmente utilizada para la tecnología 4G.
- Banda 2100 MHz o banda 1. Utilizada para 3G desde su licitación.
- Banda 2600 MHz o banda 7. Utilizada para 4G y se usará como complemento al despliegue del 5G en la banda 42.
- Banda 3500 MHz o banda 42. Banda principal de los servicios 5G.
- Banda 26 GHz. Banda 5G que ofrece mayor velocidad pese al corto alcance.

La Figura 3.3 muestra dichas bandas y los MHz ocupados por operador.

	800 MHz 4G banda 20	**900 MHz** 2G/3G banda 8	**1800 MHz** 2G/4G banda 3	**2100 MHz** 3G banda 1	**2600 MHz** 4G banda 7	**3500 MHz** 5G banda 42
Movistar	10 MHz	14,8 MHz	20 MHz	15 MHz FDD 5 MHz TDD	20 MHz	90 MHz
Vodafone	10 MHz	10 MHz	20 MHz	15 MHz FDD 5 MHz TDD	20 MHz FDD 20 MHz TDD	90 MHz
Orange	10 MHz	10 MHz	20 MHz	15 MHz FDD 5 MHz TDD	20 MHz	100 MHz
MásMóvil			14,8 MHz	15 MHz FDD 5 MHz TDD	10 MHz TDD (autonómicos)	80 MHz

Figura 3.3 Bandas de frecuencias por operador [37].

3.4 Protocolos de red y envío de IMSI

En los apartados anteriores se han expuesto los fundamentos de la tecnología móvil a partir de los cuales, a continuación, se desarrollarán los métodos de cifrado y verificación de las redes GSM, UMTS y LTE que permiten la captura de IMSI.

3.4.1 GSM (2G)

La arquitectura de seguridad de las redes GSM trata de proveer de servicios como el anonimato de la identidad del usuario, la autenticación de los dispositivos, la confidencialidad de los datos de usuario y la utilización de la tarjeta SIM como módulo de seguridad.

La tarjeta SIM es una tarjeta criptográfica que incluye toda la información para acceder a la cuenta del usuario. En cada tarjeta se almacenan el IMSI y el *Individual subscriber authentication Key* (Ki), un número aleatorio de 128 bits que se utiliza como clave criptográfica para generar claves de sesión y autenticar a los usuarios. El Ki únicamente se encuentra en la tarjeta SIM de cada dispositivo y en el centro de autenticación de la operadora.

La confidencialidad y seguridad de los usuarios están en manos de estos dos valores, conociéndolos es posible hacerse pasar por otra persona. En la SIM se implementan también los algoritmos de seguridad A3 y A8, el primero utilizado para autenticar usuarios y el segundo para encriptar las claves de sesiones.

El protocolo de conexión se denomina *Subscriber Identity Authentication* (SIA) y es el siguiente [38]:

1. Cuando una estación móvil pide acceso a la red, la estación de control (MSC) pedirá que el dispositivo se identifique a partir del IMSI. El MSC pasará el IMSI al *Home Location Register* (HLR), una base de datos que contiene la información de subscripción de los abonados.

2. Cuando el HLR recibe el IMSI y la petición de autenticación, primero comprueba que dicho identificador se encuentra en la base de datos. Si la verificación es correcta, pasa el IMSI al centro de autenticación (*Authentication Center* (AuC)).

3. El AuC utiliza el IMSI para buscar el Ki asociado a él. También genera un número aleatorio de 128 bits llamado RAND.

4. El RAND y el Ki se toman como valores de entrada para el algoritmo de encriptación A3. La salida es el número de 32 bits *Signed Response* (SRES).

5. Así mismo, el RAND y el Ki son utilizados como entrada del algoritmo A8, que generará como salida el Kc de 64 bits. RAND, SRES y Kc son conocidos como *Triplets* (trillizos) y se mandan como respuesta del AuC al HLR y del HLR a la estación de control. Cada set de *triplets* es único para un IMSI.

6. El MSC (estación de control) almacena el Kc y SRES y envía el RAND al dispositivo móvil para que verifique su identidad. Puesto que la SIM almacena los algoritmos A3 y A8, utiliza el IMSI y el RAND recibido para generar Kc y SRES y enviarlo al MSC.

7. La estación de control compara los valores recibidos del dispositivo móvil con los generados por el centro de autenticación. Si coinciden, el dispositivo se conecta correctamente.

Los envíos del dispositivo móvil al centro de control se hacen a través de la estación base más cercana. Capturando los paquetes a la frecuencia de dicha estación base el IMSI es detectado en el paso 1 del proceso de conexión cuando el dispositivo hace la primera comunicación con la red.

3.4.2 UMTS (3G) y LTE (4G)

A diferencia de su predecesor, los protocolos utilizados tanto para UMTS como LTE se denominan *Authentication and Key Agreement* (AKA). El protocolo es muy similar para las dos tecnologías, por lo que se desarrollarán juntas. Existen tres partes involucradas en el protocolo [30]:

- Equipo de usuario (*User Equipment*) (UE). Dispositivo con el que se realiza la conexión (teléfono, PC, etc) y la *Universal Subscriber Identity Module* (USIM), similar a la SIM de GSM. Contiene el IMSI, la clave de subscripción permanente (K) y los algoritmos criptográficos utilizados. Además mantiene un número de secuencia SQN_U.

El núcleo de conexión, externo al dispositivo móvil, se divide en *Service Network* y *Home Network*.

- *Service Network* (SN): es el responsable de la comunicación entre el equipo de usuario y la red. En UMTS equivale sl SGSN y en LTE al MME. Contiene el identificador del SN.

- *Home Network* (HN): contiene y gestiona el centro de autenticación (AuC). En UMTS equivale al HLR (al igual que en GSM) y en LTE a *Home Subscriber System* (HSS). Es una base de datos que conoce la información de autenticación (IMSI y K) de todos los usuarios así como los algoritmos de encriptación. En el caso de LTE, también comparte con el usuario una función de derivación de clave (*Key Derivation Function* (KDF)). Mantiene su propio número de secuencia SQN_H

Conociendo las partes que componen el sistema, se describen las fases del protocolo [39].

1. El equipo de usuario (UE) inicia el protocolo enviando una petición de conexión al SN, que envía a su vez una petición de iniciación de autenticación (*Authentication Initiation Request* (AIR)) al HN. Esta petición contiene el IMSI del usuario y el identificador del SN (*SNid*).

2. HN genera un vector de autenticación (AV) y lo envía al SN. Dicho vector está formado por un número aleatorio RAND y los códigos generados por la AuC a partir del RAND, clave K asociada al IMSI del usuario y el número de secuencia SQN_H: *Message Autorization Code* (MAC) (codigo de autorización de mensaje), *Expected Response* (XRES) (respuesta esperada) y *Authentication Token* (AUTN) (token de autenticación). En UMTS se incluyen en el vector la *Cipher Key* (CK) (clave de cifrado) y *Integrity Key* (IK) (clave de integridad) y en su lugar, LTE se genera la clave de sesión *Skey*.

3. A continuación SN envía al usuario una petición de autenticación de usuario, acompañado del RAND y AUTN. El usuario extrae SQN_H, calcula el *Expected Message Authentication Code* (XMAC) (codigo de autorización de mensaje esperado) y lo compara con el MAC contenido en AUTN. Si coinciden, comprueba que los números de secuencia SQN_U y SQN_H sean iguales. En el caso de que alguna de las dos comprobaciones falle, envía un mensaje de error a SN. Si

ambas son correctas el usuario computa la respuesta RES y la envía a SN. La red de servicio compara RES con la respuesta esperada XRES recibida de HN, si coinciden la conexión se completa correctamente.

Al igual que en GSM la conexión entre el equipo de usuario y la red de servicio (SN) se realiza a partir de las estaciones base (NodeB para 3G y eNodeB para 4G), por lo que los IMSIs son capturables a la frecuencia de dichas estaciones durante la primera conexión en el paso 1.

3.4.3 5G

Para evitar la captura de IMSI, la tecnología 5G sustituye dicho identificador por el *Subscriber Permanent Identifier* (SUPI). Por tanto, en el momento que el soporte principal de la red se base en 5G, el modelo propuesto será menos eficaz, limitándose a los dispositivos que continúen utilizando 3G y 4G.

Destacar también que 5G también sigue un protocolo AKA, aunque añadiendo una verificación más a nivel de HN, como se aprecia en la Figura 3.4.

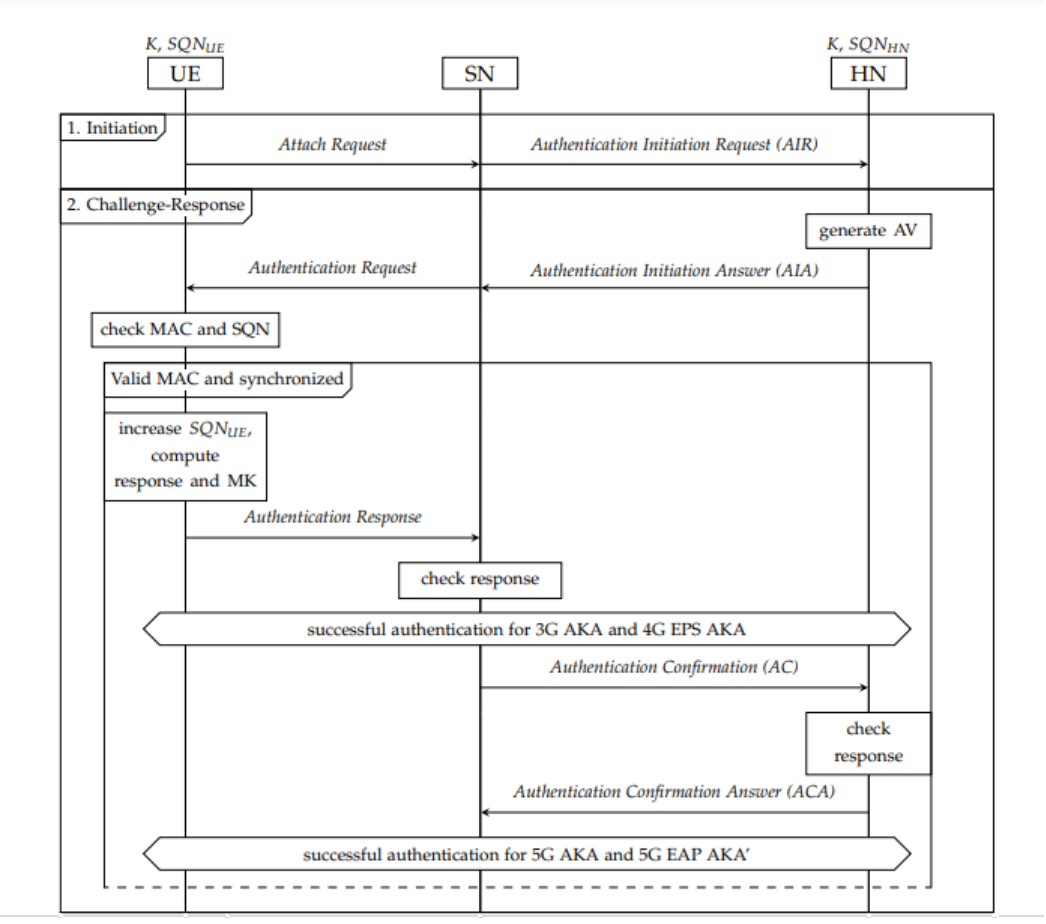

Figura 3.4 Fases generales del protocolo AKA [40].

3.5 Hardware y Software elegidos

Para el desarrollo del prototipo, son necesarios el uso de un hardware y un software específicos, que se detallan a continuación.

3.5.1 Hardware

Se define un *Software Defined Radio* (SDR) (Radio Definida por Software), como la radio en la que alguna o todas las funciones del hardware (filtros, moduladores, demoduladores, etc) están implementadas por software.

El sistema típico consiste en un receptor de ondas de radiofrecuencia y un convertidor analógico digital (ADC), convirtiéndolo en un hardware muy económico [41]. Para el prototipo a desarrollar, las variables fundamentales según las cuales elegir un dispositivo u otro son el rango de frecuencias que es capaz de recibir y el precio. Comparando las opciones disponibles en el mercado, buscando que incluyan antenas para aumentar el rango de detección se dan tres posibilidades:

- *RTL-SDR* [42]. Rango de frecuencias comprendido desde 500 kHz hasta 1.75 GHz. Precio 39.97€.
- *Nooelec NESDR SMArtee XTR* [43]. Rango de frecuencias entre 500 kHz y 2.35 GHz. Precio 52.95€.
- *HackRF One* [44]. Frecuencia operativa entre 1 MHz y 6 GHz. Funciona tanto como receptor como transmisor y es posible hacer dos lecturas simultáneas. Precio 329.95€.

Si se comparan los rangos de frecuencias con las bandas vistas en el apartado 3.3 se observa que el primer dispositivo solo es capaz de detectar las bandas 20 (800 MHz) y 8 (900 MHz), mientras que el segundo admite además las bandas 3 (1800 MHz) y 1 (2100 MHz). El tercero no tiene ninguna limitación de frecuencia.

Por ello, dado que se trata de un prototipo, se considera que la mejor opción será utilizar el dispositivo de *Nooelec* pese a no llegar a los 2600 MHz, pero siendo una opción mucho más económica que la tercera.

Además del SDR, con un conector USB y un MCX macho para la antena, se incluye una antena telescópica y dos fijas de 4.5" y 10.5", además de una base para dichas antenas.

3.5.2 Software

El software específico utilizado se detalla a continuación.

- GNU radio [45]. Se trata de un proyecto de código abierto (*open source*) que proporciona librerías y bloques para desarrollar radios software. Permite tanto controlar hardware externo como sin hardware, realizando simulaciones teóricas. Se utiliza en el sistema operativo Linux, y aunque su uso no es obligatorio, facilita la integración del componente hardware.

- Gr-gsm [46]. Conjunto de paquetes desarrollados para GNU radio que procesan transmisiones de la red telefónica. Desarrollada en un principio para GSM y ampliada a UMTS y LTE a posteriori.

- Wireshark [47]. Software analizador de protocolos utilizado para realizar análisis de redes de comunicaciones. Permite capturar los paquetes recibidos y posee una amplia gama de filtros que facilitan la búsqueda de la información deseada.

- PostgreSQL [48]. Base de datos de código abierto. Utilizada para almacenar y organizar los datos extraídos.

En el siguiente capítulo se detalla el conjunto de pruebas realizadas con las herramientas descritas, así como los resultados obtenidos a partir de ellas.

4 Validación experimental

En este capítulo se contemplan los distintos aspectos del desarrollo del prototipo, así como de las pruebas realizadas con él, comenzando con la puesta en marcha del dispositivo hardware, siguiendo con la elección de estaciones base, captura de paquetes y con la posibilidad de estimar la posición de los dispositivos a partir de las lecturas obtenidas. Por último, se elaboran las estadísticas extraídas de los datos recogidos durante varios días, procesados a partir de una base de datos.

4.1 Instalación y puesta en marcha

Tal y como se explica en el apartado 3.5, el hardware elegido es el receptor *Nooelec NESDR Smartee XTR*, cuya imagen se presenta en la Figura 4.1. Antes de comenzar a recoger datos es necesario instalar todas las librerías y paquetes necesarios, así como probar que el dispositivo funciona correctamente.

Figura 4.1 Hardware utilizado para el prototipo (Nooelec NESDR Smartee XTR).

Todo el software utilizado forma parte de los programas *GNU Radio* y *gr-gsm*, programas específicos para procesamiento de señales de radiofrecuencias y de transmisiones de telefonía respectivamente. Ambos funcionan sobre el sistema operativo *Ubuntu*, en este caso con la versión 16.04.

La prueba más simple a realizar se trata de si el ordenador detecta el hardware correctamente. Para ello se ejecuta el comando `rtl_test`, obteniendo como salida las propiedades del dispositivo, como se observa en la Figura 4.2.

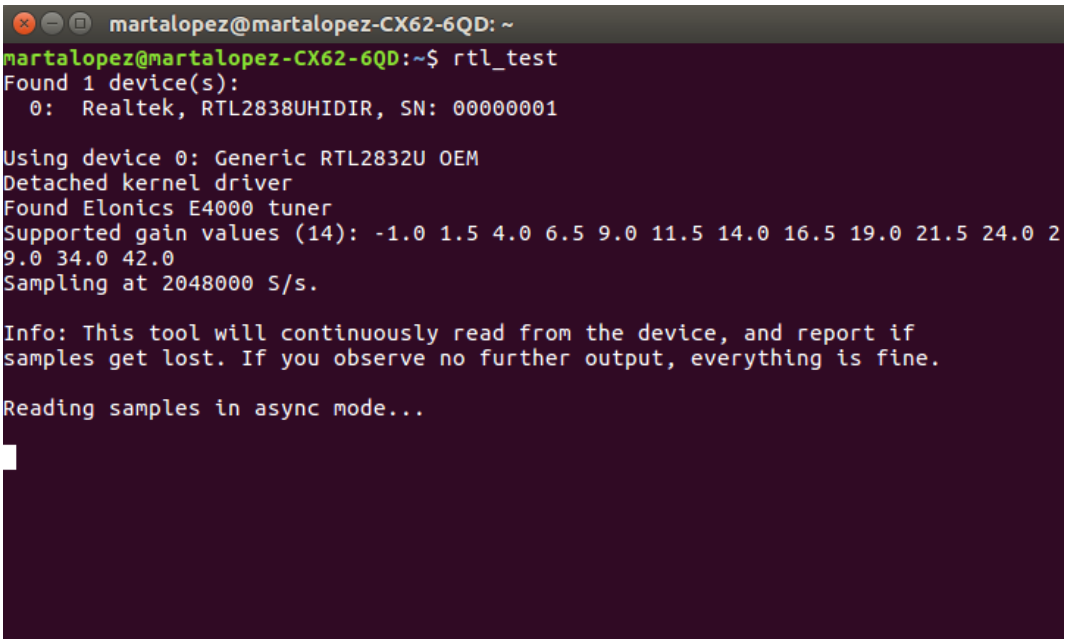

Figura 4.2 Puesta en marcha del dispositivo.

Tras comprobar que en efecto, el dispositivo es detectado, el siguiente paso es tratar de recibir información de una frecuencia determinada. Para ello, dentro de *GNU Radio* se encuentra el programa `gqrx`, que permite elegir la frecuencia de detección, ganancia, desmodulación (AM, FM, etc), entre otros parámetros.

Puesto que las emisoras de radio FM se encuentran dentro del rango de acción del receptor SDR y la comprobación de su recepción es sencilla, se intenta sintonizar una de estas. La elegida, *Los 40 Sevilla* emite a una frecuencia de 97.1 MHz y con los parámetros de la Figura 4.3, es posible escucharla.

Además, se pueden apreciar en la imagen las frecuencias a las que existen emisoras, siendo las zonas en las que la potencia de la señal es mayor. Así, se puede suponer que a 96.5 MHz existe una, coincidiendo con la frecuencia a la que emite *Máxima FM*.

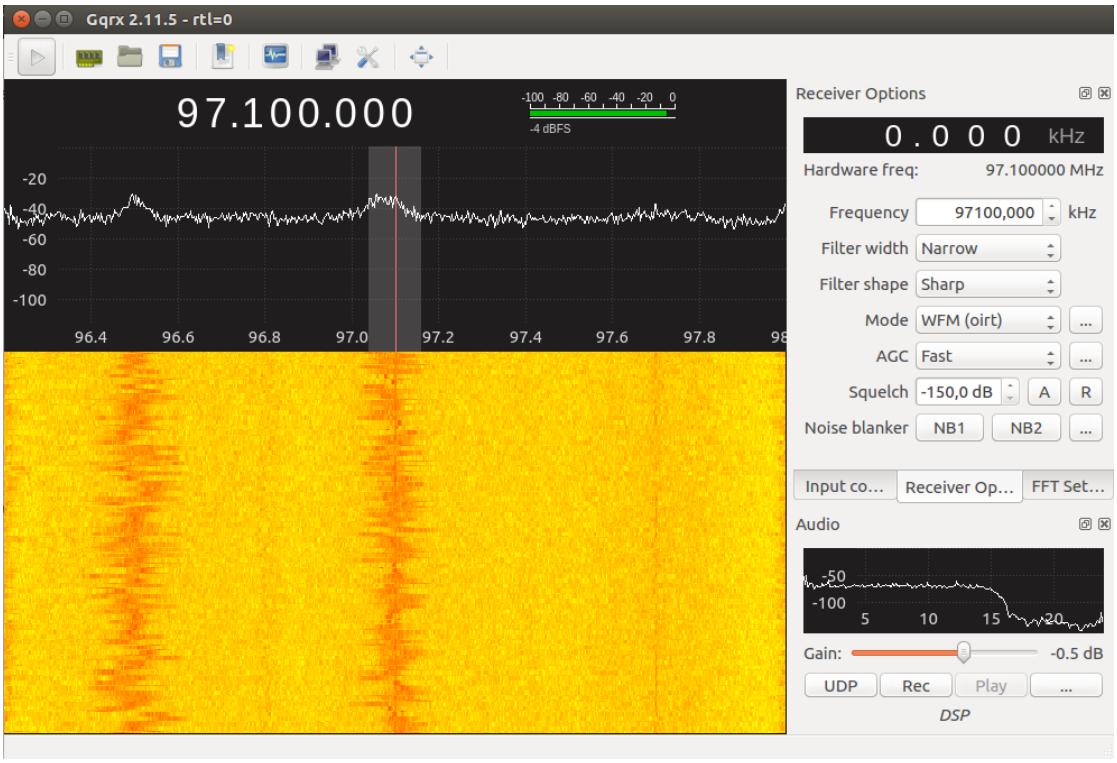

Figura 4.3 Recepción de señal de radiofrecuencia.

La última prueba a realizar para concluir la puesta en marcha del hardware y software necesario para su funcionamiento, es buscar estaciones base cercanos al dispositivo. Para ello se utiliza la ya mencionada herramienta *gr-gsm*.

Por un lado, el comando `grgsm_scanner -h` muestra las opciones de bandas, tasa de muestreo, ganancias o dispositivos receptores, como se muestra en la Figura 4.4.

```
martalopez@martalopez-CX62-6QD: ~
martalopez@martalopez-CX62-6QD:~$ sudo grgsm_scanner -h
[sudo] password for martalopez:
linux; GNU C++ version 5.4.0 20160609; Boost_105800; UHD_003.010.003.000-0-unkno
wn

Usage: grgsm_scanner: [options]

Options:
  -h, --help            show this help message and exit
  -b BAND, --band=BAND  Specify the GSM band for the frequency. Available
                        bands are: GSM900, DCS1800, GSM850, PCS1900, GSM450,
                        GSM480, GSM-R
  -s SAMP_RATE, --samp-rate=SAMP_RATE
                        Set sample rate [default=2000000.0] - allowed values
                        even_number*0.2e6
  -p PPM, --ppm=PPM     Set frequency correction in ppm [default=0]
  -g GAIN, --gain=GAIN  Set gain [default=24.0]
  --args=ARGS           Set device arguments [default=]. Use --list-devices
                        the view the available devices
  -l, --list-devices    List available SDR devices, use --args to specify
                        hints
  --speed=SPEED         Scan speed [default=4]. Value range 0-5.
  -v, --verbose         If set, verbose information output is printed: ccch
                        configuration, cell ARFCN's, neighbour ARFCN's
  -d, --debug           Print additional debug messages
martalopez@martalopez-CX62-6QD:~$
```

Figura 4.4 Configuración del receptor de señales de telefonía.

Por último el comando `grgsm_scanner -b GSM900` devuelve los parámetros de todas las estaciones base encontradas alrededor, como se muestra en la Figura 4.5. Dichos parámetros que definen a la estación base son:

- *Absolute Radio-Frecuency Channel Number* (ARFCN). Código único que se le da a cada canal de la red de telefonía.
- Frecuencia a la que emite la estación base.
- *Cell ID* (CID). Número que identifica a cada estación base en una región.
- *Location Area Code* (LAC). Número que identifica un área, siendo un área un conjunto de estaciones base agrupados para mejorar la señal.
- MCC Código de identificación del país. En España es el 214.
- MNC Código de identificación de la operadora. Las principales operadoras españolas se identifican con los siguientes MNC:
  - 01 - Vodafone
  - 03 - Orange
  - 04 - Yoigo
  - 07 - Movistar
- Potencia de la señal recibida.

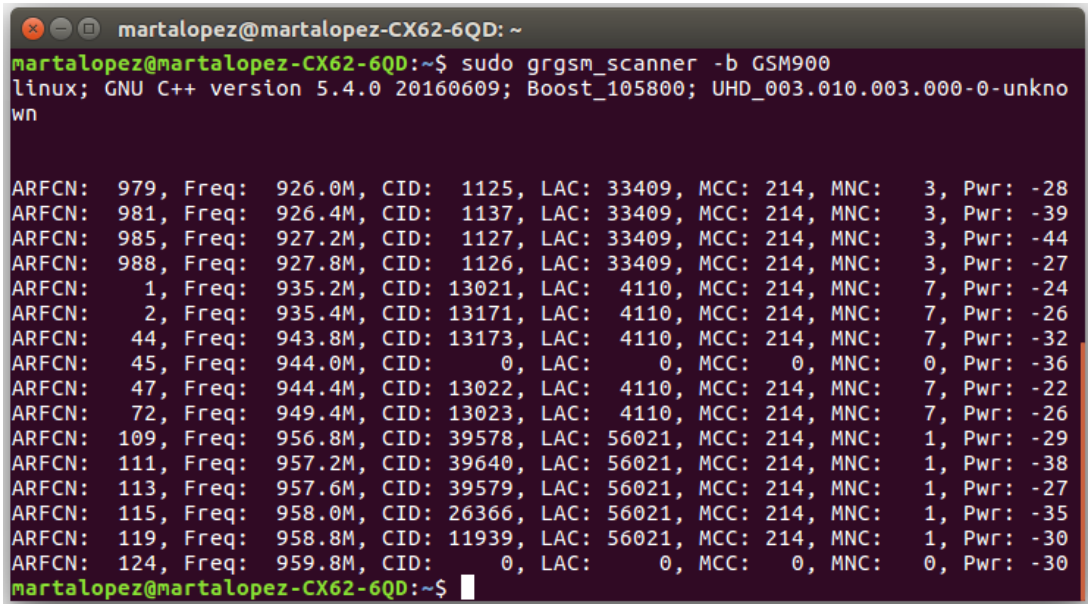

Figura 4.5 Búsqueda de estaciones base cercanas.

A continuación, se desarrolla la elección de la estación base deseada.

4.2 Elección de estación base

Anteriormente se ha expuesto el procedimiento seguido para encontrar las estaciones base cercanas al dispositivo hardware. No obstante, el principal interés no reside en recibir las señales de una estación aleatoria, sino elegir aquellas que cubren el área deseada.

Para ello es necesario una base de datos que contenga todas las estaciones de la zona, así como sus identificadores CID, LAC y MNC o su frecuencia de recepción.

Se encuentran 3 fuentes de datos, dos actualizadas por radioaficionados: *OpenCell Id* [49] y *CellMapper* [50] y una tercera mantenida por el Ministerio de Asuntos Económicos y Transformación Digital [51]. Sin embargo, los datos de estas no siempre coinciden.

Se expone el caso de la Escuela Técnica Superior de Ingeniería de Sevilla, donde la fuente del Ministerio indica un nodo de tres operadoras (Figura 4.6), que al desglosar una de ellas se observa que cubre las bandas 20, 8, 3, 1 y 7, como se aprecia en la Figura 4.7.

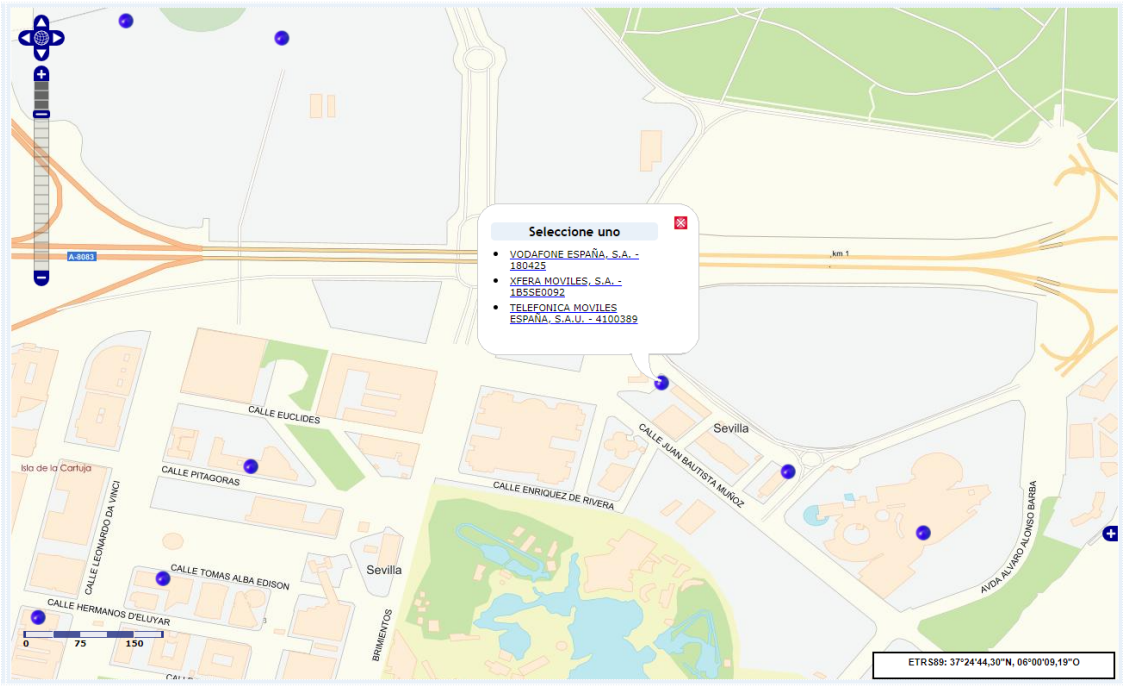

Figura 4.6 Mapa estaciones cercanas a la Escuela según el Ministerio de Asuntos Económicos [51].

En esta fuente se obtiene información fiable de la localización de algunas estaciones base, aunque los datos recogidos no sean suficientes para identificar dichos nodos con el dispositivo. Para ello, las otras dos fuentes aportan más información.

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO PARA LA SOCIEDAD DE LA INFORMACIÓN Y LA AGENDA DIGITAL · Infoantenas

ESTACIONES DE TELEFONÍA MÓVIL

LOCALIZACIÓN

Código	Dirección
VODAFONE ESPAÑA, S.A. - 180425	CL JUAN BAUTISTA MUÑOZ ED.FLOTA EXPO, S/N. SEVILLA, SEVILLA

CARACTERISTICAS TÉCNICAS

Operador	Referencia	Banda Asignada (MHz)
VODAFONE ESPAÑA, S.A.	SESE-1800020	949.90 - 959.90
VODAFONE ESPAÑA, S.A.	SESE-1800021	842.00 - 852.00
VODAFONE ESPAÑA, S.A.	SESE-1800022	1825.10 - 1845.10
VODAFONE ESPAÑA, S.A.	SESE-1800023	2660.00 - 2680.00
VODAFONE ESPAÑA, S.A.	SESE-1800025	1905.00 - 1910.00; 2140.00 - 2155.00
VODAFONE ESPAÑA, S.A.	SESE-2000138	2140.00 - 2155.00
VODAFONE ESPAÑA, S.A.	SESE-1800024	949.90 - 959.90

NIVELES MEDIDOS EN EL ENTORNO

Distancia (m)	(*) Acimut (º)	Valor Medido (µW/cm²)
63.0	20.0	0.61285
98.0	110.0	0.28690
75.0	255.0	0.74866
85.0	295.0	1.10390
76.0	350.0	0.70476

Figura 4.7 Desglose estación Vodafone cercana a la Escuela según el Ministerio de Asuntos Económicos [51].

La web *OpenCell Id* (Figura 4.8) muestras las estaciones en una localización similar al Ministerio y otras muchas más, aunque no todas actualizadas recientemente. Esta plataforma si ofrece los parámetros identificativos que asegurarían la correcta recepción del nodo deseado.

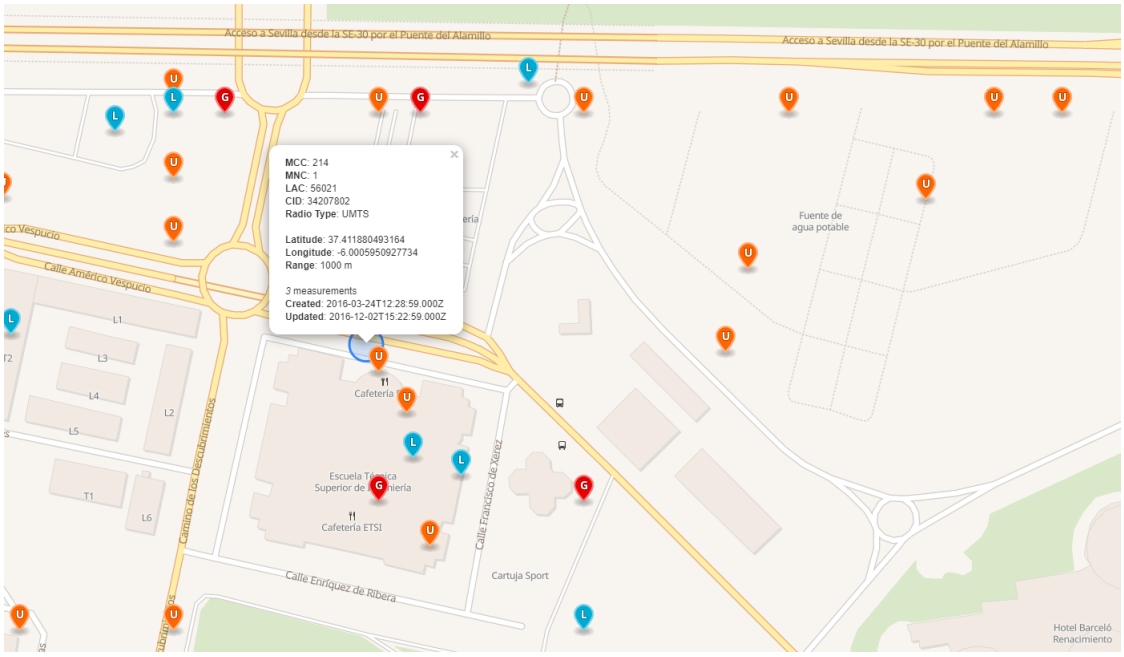

Figura 4.8 Mapa estaciones cercanas a la Escuela según *OpenCell Id* [49].

Al ser páginas mantenidas por sus propios usuarios, sus datos no siempre son exactos o están actualizados. Esto se observa al comprobar la misma zona en la base de datos de *CellMapper* (Figura 4.9), donde para ninguna operadora ni banda aparecen estaciones base existentes.

Figura 4.9 Mapa estaciones cercanas a la Escuela según *CellMapper* [50].

En zonas de densidad de población más alta, los datos obtenidos con las dos páginas no oficiales son más precisos. Considerando el caso de una aplicación comercial real, lo ideal sería obtener información de primera mano de las operadoras, conociendo con exactitud los parámetros y rangos de las estaciones base de interés.

4.3 Captura de paquetes de la red telefónica

Una vez se conocen las herramientas para posicionar las estaciones detectadas y determinar la deseada, llega el momento de la recepción de datos. Para ello se hace uso del comando `sudo grgsm_livemon -f` al que se añade la frecuencia a la que se desea recibir. Como ejemplo se utiliza la estación base con CID 1126 que se encuentra en la Figura 4.5 a una frecuencia de 927.8 MHz. Al ejecutar `sudo grgsm_livemon -f 297.8M` aparece la ventana de control que se muestra en la Figura 4.10 que permite cambiar la frecuencia de captura.

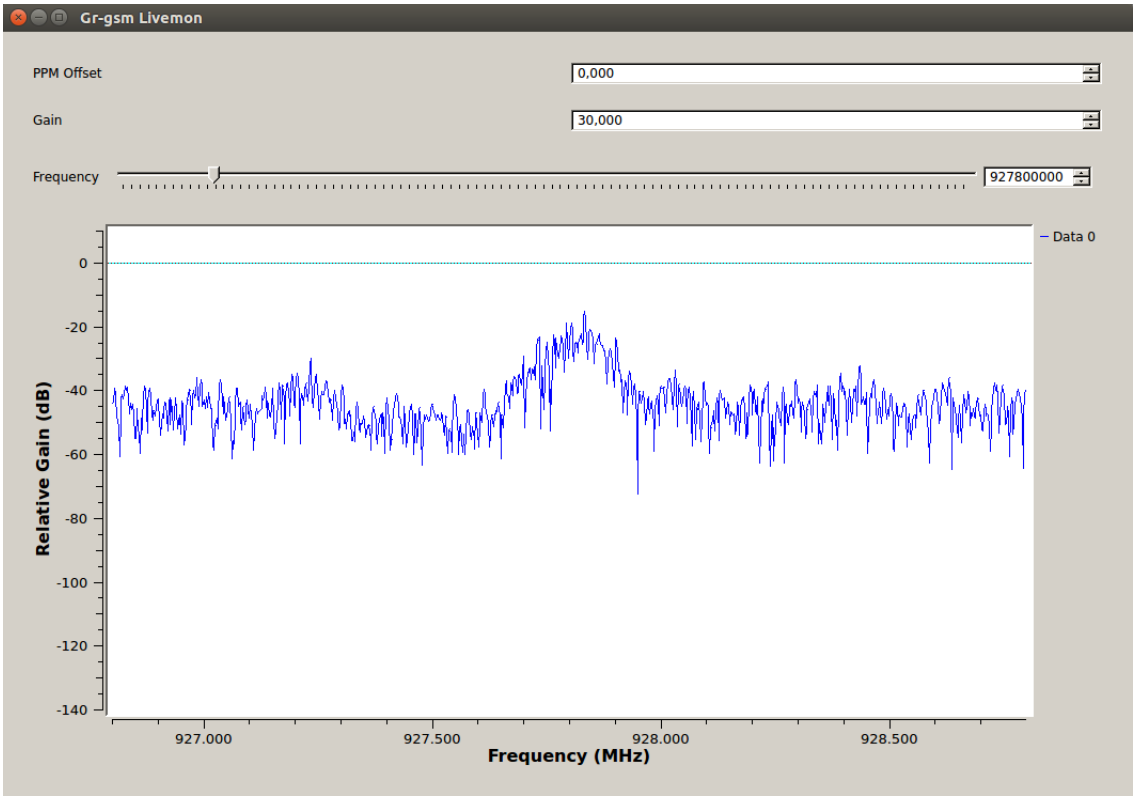

Figura 4.10 Ventana control de la frecuencia de captura.

Sin ningún procesamiento, los datos recogidos aparecen como salida de la terminal en forma de miles de datos en hexadecimal (Figura 4.11). Para su procesamiento, se utilizan dos herramientas.

La primera se trata de un *script* escrito en el lenguaje de programación *Python* el cual lee los valores hexadecimales buscando IMSIs no detectados anteriormente y los almacena en una lista. También muestra el operador y país de pertenencia en función del MCC y MNC y añade, si los hay, los TMSI asociados (Figura 4.12)

```
martalopez@martalopez-CX62-6QD: ~
martalopez@martalopez-CX62-6QD:~$ sudo grgsm_livemon -f 927.8M
[sudo] password for martalopez:
linux; GNU C++ version 5.4.0 20160609; Boost_105800; UHD_003.010.003.000-0-u
nknown

gr-osmosdr v0.1.x-xxx-xunknown (0.1.5git) gnuradio 3.7.10
built-in source types: file osmosdr fcd rtl rtl_tcp uhd plutosdr miri hackrf
 bladerf rfspace airspy airspyhf soapy redpitaya
Using device #0 Realtek RTL2838UHIDIR SN: 00000001
Found Elonics E4000 tuner
Exact sample rate is: 2000000,052982 Hz
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 b9 b6 ed 1b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 a1 b5 58 92 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 31 06 1c 12 f4 30 82 81 65 44 78 00 00 80 00 b2 2b 2b 2b 2b 2b 2b 2b
 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 2d 06 22 f0 48 d8 87 63 a8 c6 d4 3b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 33 cf 83 49 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 00 05 f4 df 30 59 06 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 01 06 00 d0 10 18 78 65 4a 92 a5 3b 29 42 db 2b 2b 2b 2b 2b 2b 2b 2b
 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 09 bf da 76 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 b9 b6 ed 1b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 31 cf db 7e 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 a1 b5 58 92 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 81 c0 c1 4e 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 49 06 03 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2b 2b 2b 2b
 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
```

Figura 4.11 Salida de la terminal al capturar señales.

Nb IMSI	TMSI-1	TMSI-2	IMSI	country	brand	operator	MCC	MNC	LAC	CellId	Timestamp
1			214 04 2695087272	Spain	Yoigo	Xfera Moviles SA	214	03	33409	1126	2021-06-02T17:35:29.568643
2			214 03 9084007810	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:35:35.013377
3			214 04 2800649885	Spain	Yoigo	Xfera Moviles SA	214	03	33409	1126	2021-06-02T17:35:36.263505
4			214 03 1785160928	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:35:39.002869
5	0xc0286606		214 03 5847800553	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:35:50.076424
6			214 03 5070859750	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:35:56.303966
7			208 01 6802853467	France	Orange	Orange S.A.	214	03	33409	1126	2021-06-02T17:35:57.413798
8			214 03 3080186679	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:35:58.465077
9			214 03 6585035612	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:35:59.780247
10			214 03 5036364150	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:35:59.839788
11			214 03 3885283371	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:36:00.698762
12			214 04 0113888197	Spain	Yoigo	Xfera Moviles SA	214	03	33409	1126	2021-06-02T17:36:01.219736
13			214 03 5849306209	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:36:06.785189
14			214 04 2002087148	Spain	Yoigo	Xfera Moviles SA	214	03	33409	1126	2021-06-02T17:36:12.496038
15	0x06c8ec23		286 01 6838308051	Turkey	Turkcell	Turkcell Iletisim Hizmetleri A.S.	214	03	33409	1126	2021-06-02T17:36:13
16			214 03 3582018057	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:36:18.782040
17			214 03 5036483291	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:36:19.050098
18			214 03 3773080692	Spain	Orange	Orange Espagne S.A.U	214	03	33409	1126	2021-06-02T17:36:20.970167
19			214 04 0116180956	Spain	Yoigo	Xfera Moviles SA	214	03	33409	1126	2021-06-02T17:36:26.851287

Figura 4.12 Salida del *script* de *Python* desarrollado para encontrar IMSIs únicos.

Por otro lado, se encuentra el ya mencionado software *Wireshark* que captura y decodifica las entradas hexadecimales de la terminal, convirtiéndolas a paquetes fácilmente analizables. Cuenta además con filtros que permiten mostrar únicamente los paquetes de telefonía o aquellos que contienen IMSIs.

Analizando los mensajes recibidos y utilizando el filtro `e212.imsi` se observa que aquellos paquetes de tipo *Paging Request Type x* son los que contienen identificadores (Figura 4.13).

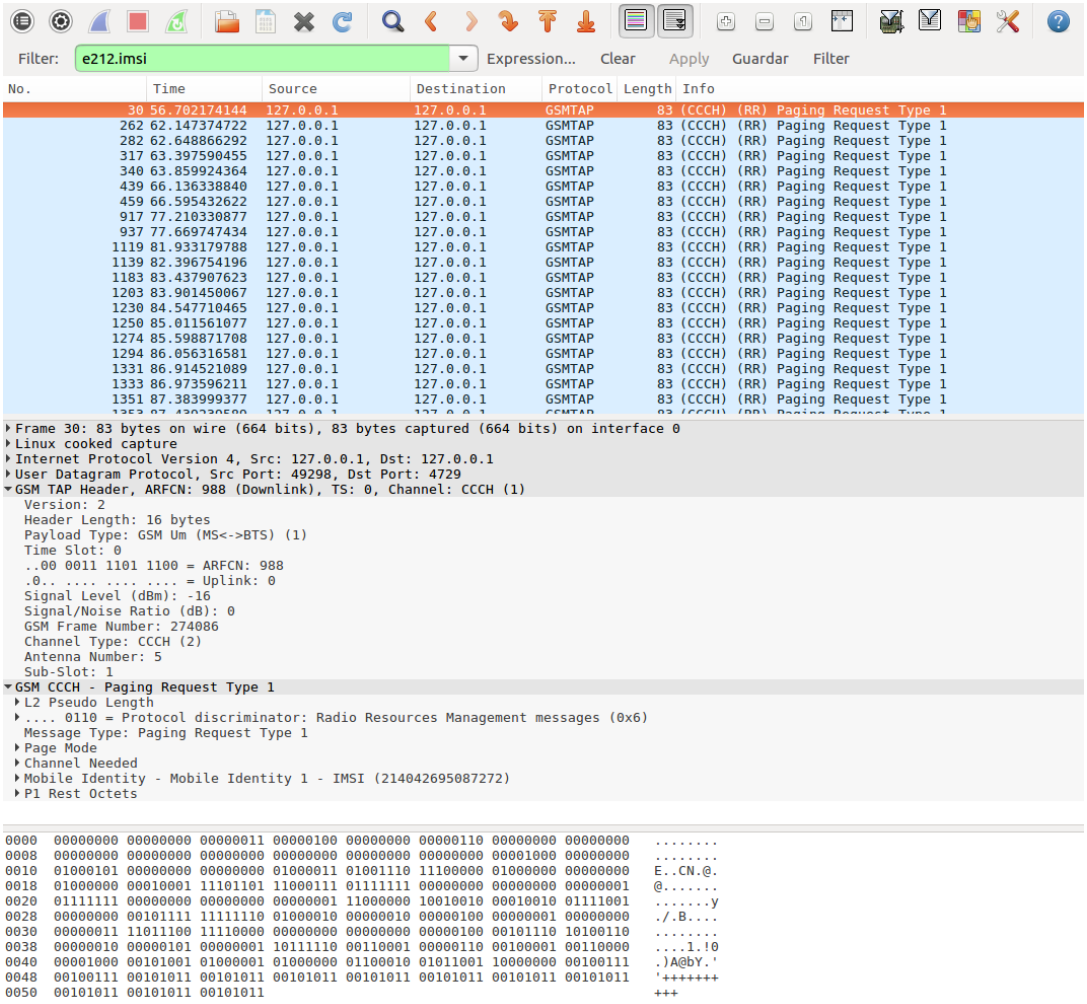

Figura 4.13 Tráfico capturado en *Wireshark* con filtros de IMSI.

Entre otros datos captados destacan la marca de tiempo, que registra la fecha y hora exactas de llegada con precisión de millonésimas de segundo, y la potencia de la señal recibida (en dBm). Este último hace preguntarse si es posible estimar la distancia del dispositivo leído a la estación base, obteniendo datos de posicionamiento además de conteo y periodicidad.

Todos los paquetes capturados en *Wireshark* son fácilmente exportables a otros formatos para procesar la información obtenida.

4.4 Posicionamiento de dispositivos

Como se mencionó en el apartado anterior, el conocimiento de la potencia de señal recibida, junto a la posición y orientación de la antena en la estación base o nodo, puede dar lugar al posicionamiento de los dispositivos detectados.

Dentro de la amplitud de tipos de redes inalámbricas, los métodos de posicionamiento son limitados. Pueden depender de las identidades externas de las estaciones base o de propiedades dependientes como el *Received Signal Strength* (RSS) [52].

Cell ID

La identificación de celdas, también llamada *Cell ID* estima la localización de los dispositivos a partir de la localización de las estaciones base a las que están conectados. Se toma la posición de la base como un punto de referencia fijo y se asigna dicha posición a cada uno de las estaciones móviles conectadas.

La precisión de este método está limitada por el rango de comunicación de la estación base. En casos de corto rango, como módulos WiFi puede limitarse a decenas de metros, mientras que con la red de telefonía pueden llegar a ser miles.

En el caso de la aplicación, la identificación de celdas no aporta información relevante sobre la posición de los dispositivos, ya que la estación base es elegida previamente por su posición.

Tiempo de llegada

El tiempo de llegada es la marca de tiempo del reloj interno del receptor cuando llega una señal. Se puede estimar la distancia entre un par de nodos A y B, utilizando la medida del retardo de propagación de la señal o tiempo de vuelo. Este cálculo puede realizarse mediante el tiempo de ida, el tiempo de ida y vuelta o la diferencia de tiempo de llegada.

- **Tiempo de ida**: siendo t_1 la marca de tiempo en la que A envía un paquete, que contiene dicha marca, t_2 la marca de tiempo en la que B lo recibe y siendo la velocidad de propagación de las ondas electromagnéticas en el aire $c \simeq 3 * 10^8 m/s$, se define la distancia entre ambos puntos como:

$$d_{AB} = (t_2 - t_1) * c \tag{4.1}$$

- **Tiempo de ida y vuelta**: en el caso de que la referencia de tiempo tenga que ser común, es posible calcular la distancia entre A y B como el tiempo en el que tarda en ir de A a B, junto al tiempo de procesamiento t_D y el tiempo de enviar la respuesta de B a A.

$$d_{AB} = (2 * (t_2 - t_1) + t_D) * c \tag{4.2}$$

  Este tipo de medición es altamente dependiente de cualquier pequeño offset durante el procesamiento de la señal, causando errores por acumulación en t_D.

En el caso de saber con seguridad que dos paquetes capturados consecutivos pertenecen a la comunicación entre el mismo dispositivo móvil y la estación base de la que se recibe, sería posible calcular la distancia. Puesto que solo algunos de los mensajes incluyen identificador, es imposible comprobar la procedencia de todos los mensajes y por tanto el posicionamiento.

- **Diferencia de tiempo de llegada**: se calcula mediante dos o más medidas de tiempo de ida y puede realizarse tanto por el receptor como por el transmisor. En modo receptor, dos o más estaciones base de localización conocida retransmiten una señal sincronizada hacia el dispositivo móvil. El móvil calcula sus tiempos de ida y estima su posición triangulando los tiempos de ida, similar al funcionamiento del GPS.

  En modo transmisor, el dispositivo envía señales a balizas (estaciones base), que comparten sus tiempos de ida y calculan la posición del móvil (Figura 4.14).

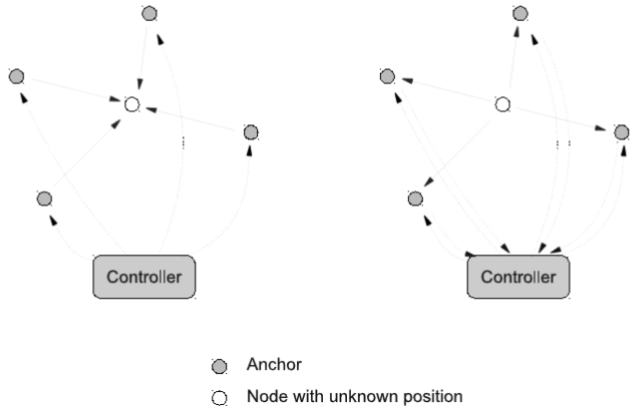

Figura 4.14 Modo transmisor y receptor de la Diferencia de Tiempo de Llegada [53].

Pese a ser mucho más preciso que los dos anteriores, no se dispone de control sobre los dispositivos móviles ni las estaciones base para enviar señales, por lo que no es implementable.

De los métodos basados en tiempos de llegada, el único aplicable al prototipo desarrollado es el primero. No obstante, debido al amplio rango que cubre cada estación base y a la existencia de interferencias entre el punto de emisión y recepción, la incertidumbre de la medida sería mayor que la medida en sí. Esta técnica podría dar resultados más exactos en zonas rurales donde el error por rebote de la señal es menor que en zonas urbanas con multitud de edificios.

Potencia de señal

La fuerza de la señal (RSS) es la magnitud de la potencia de la señal que el receptor percibe.

El RSS puede definirse con una componente constante modelada por el *path loss* o pérdida en trayectoria y una componente variable modelada por una serie de efectos de propagación: atenuación de señal, desvanecimiento lento (*shadowing*), efectos multi-trayectoria, dispersión y difracción [52].

Para el modelo de pérdida de trayectoria se considera la siguiente ecuación:

$$p = \alpha - 10\beta log(d) \tag{4.3}$$

Donde p es la potencia de señal recibida, α depende de la potencia de transmisión y pérdidas y componentes del sistema, β es el exponente de pérdida de trayectoria y d es la distancia de la comunicación. La componente variable es difícil de estimar ya es altamente dependiente del escenario en cuestión, por lo que se suele incorporar como un ruido gaussiano de desviación estándar σ. Así, la ecuación final resulta:

$$p = \alpha - 10\beta log(d) + \mu, \qquad \mu \sim Norm(0,\sigma) \tag{4.4}$$

Para convertir el RSS a distancia es necesario conocer al menos las características de propagación (β) y la potencia de transmisión real (tras las pérdidas). Incluso con todos los datos, en la práctica, la presencia de efectos de propagación hace que la onda de radio no coincida con lo calculado, resultando en medidas poco precisas.

En la realidad, la falta de datos reales de las estaciones base (altura de la antena, rango, potencia) dificulta aún más el cálculo de la distancia de manera precisa.

Por todo esto, se decide no incluirlo en el desarrollo del prototipo, ya que no se puede asegurar que las medidas obtenidas tengan la precisión necesaria para aportar información relevante.

4.5 Estudio de Periodicidad

Tras conocer el funcionamiento del hardware y el software, se realizan capturas de datos durante varios días consecutivos y no consecutivos, con el fin de estudiar el potencial real del dispositivo. Dado que la opción de implementarlo 24 horas en un centro comercial es inviable, se opta por tomar capturas de duración de 30 minutos cada una, realizándose la mitad en la banda de 1800 MHz (4g) y la otra mitad en 900 MHz (3G).

Todas ellas se realizan en la misma franja horaria, tanto en días laborables como en fines de semana, en una zona con alta densidad comercial y universitaria. Siendo un área muy transitada se espera obtener un elevado número de datos con posibilidad de estudiar la frecuencia de visita.

Los paquetes son capturados mediante *Wireshark* filtrados a aquellos que contengan IMSI y subidos a una base de datos de *PostgreSQL*. Los datos sin procesar (Figura 4.15) incluyen IMSI, TMSI si lo hay y la marca de tiempo del momento recibido.

TFG/postgres@PostgreSQL 13

Query Editor | Query History

```
1  SELECT id, imsi, tmsi1, tmsi2, "timestamp"
2      FROM public.raw_data;
```

Data Output | Explain | Messages | Notifications

	id [PK] integer	imsi character varying (100)	tmsi1 character varying (100)	tmsi2 character varying (100)	timestamp timestamp without time zone
1	299021	214035031221781	0x17ceb74d	[null]	2021-03-08 13:30:08.297459
2	299022	214035031221781	[null]	[null]	2021-03-08 13:30:08.762569
3	299023	214032885323360	[null]	[null]	2021-03-08 13:30:10.99884
4	299024	214035903315331	[null]	0x34c9f332	2021-03-08 13:30:11.063177
5	299025	214040119733801	[null]	[null]	2021-03-08 13:30:11.255456
6	299026	214035903315331	[null]	0x34c9f332	2021-03-08 13:30:11.561186
7	299027	214040119733801	[null]	0x34c9f332	2021-03-08 13:30:11.722416
8	299028	214031582123610	[null]	[null]	2021-03-08 13:30:12.704071
9	299029	214031582123610	[null]	0xa8b44bba	2021-03-08 13:30:13.160816
10	299030	214033530509954	[null]	0xa8b44bba	2021-03-08 13:30:13.422317
11	299031	214040121877088	[null]	[null]	2021-03-08 13:30:51.041971
12	299032	214042002879827	[null]	[null]	2021-03-08 13:30:51.103209
13	299033	214032885313881	[null]	[null]	2021-03-08 13:32:35.584734
14	299034	214040124426489	[null]	0x9ab15dbe	2021-03-08 13:32:35.80108
15	299035	214032885313881	[null]	[null]	2021-03-08 13:32:36.050448
16	299036	214040124426489	[null]	0x19d9ea8b	2021-03-08 13:32:37.226832
17	299037	214033530288831	[null]	0x19d9ea8b	2021-03-08 13:32:37.362559
18	299038	214031830597665	[null]	[null]	2021-03-08 13:32:37.690534
19	299039	214033530288831	[null]	0xc030686e	2021-03-08 13:32:37.835144
20	299040	214032885406816	[null]	0xfc48362e	2021-03-08 13:32:37.899192
21	299041	214033005324771	[null]	0xfc48362e	2021-03-08 13:32:37.969726
22	299042	214032885406816	[null]	0xfc48362e	2021-03-08 13:32:38.364815
23	299043	214033005324771	[null]	0xfc48362e	2021-03-08 13:32:38.426405
24	299044	214035847244732	[null]	[null]	2021-03-08 13:32:39.187627
25	299045	214035847244732	[null]	[null]	2021-03-08 13:32:39.655958
26	299046	214032530354362	[null]	0xe238506e	2021-03-08 13:32:40.06759
27	299047	214032530354362	[null]	0xe238506e	2021-03-08 13:32:41.031493
28	299048	214033830024603	[null]	[null]	2021-03-08 13:32:42.423678

Figura 4.15 Tabla de datos sin procesar.

A continuación, por cada conjunto de lecturas pertenecientes al mismo día, sin importar en que banda hayan sido recogidas, se recoge la primera y última aparición de cada IMSI, se calcula la duración como la diferencia entre ambas y se almacenan los datos en una nueva tabla de la base de datos (Figura 4.16).

TFG/postgres@PostgreSQL 13

Query Editor | Query History

```
1  SELECT id, imsi, first_seen, last_seen, duration
2      FROM public.processed_data;
```

Data Output | Explain | Messages | Notifications

	id [PK] integer	imsi character varying (100)	first_seen timestamp without time zone	last_seen timestamp without time zone	duration interval
1	287418	208017806533352	2021-04-25 18:31:41.308566	2021-04-25 18:31:41.308566	00:00:00
2	287419	214031001268915	2021-04-25 18:13:58.882374	2021-04-25 18:14:13.483909	00:00:14.60...
3	287420	214031080125829	2021-04-25 18:07:33.646687	2021-04-25 18:07:34.110123	00:00:00.46...
4	287421	214031530353055	2021-04-25 18:03:44.187897	2021-04-25 18:09:12.286562	00:05:28.09...
5	287422	214031591038670	2021-04-25 18:07:45.439199	2021-04-25 18:12:59.422823	00:05:13.98...
6	287423	214031630445197	2021-04-25 18:04:50.515391	2021-04-25 18:04:51.037282	00:00:00.52...
7	287424	214031685381514	2021-04-25 18:05:49.816807	2021-04-25 18:05:49.816807	00:00:00
8	287425	214031685426577	2021-04-25 18:20:36.178198	2021-04-25 18:20:36.683761	00:00:00.50...
9	287426	214031687171063	2021-04-25 18:17:49.873184	2021-04-25 18:18:20.027258	00:00:30.15...
10	287427	214031730080521	2021-04-25 18:05:07.622137	2021-04-25 18:20:49.606876	00:15:41.98...
11	287428	214031730108053	2021-04-25 18:15:02.037582	2021-04-25 18:15:02.498435	00:00:00.46...
12	287429	214031730119241	2021-04-25 18:07:48.345027	2021-04-25 18:07:48.850027	00:00:00.505
13	287430	214031782032957	2021-04-25 18:19:24.471945	2021-04-25 18:19:24.471945	00:00:00
14	287431	214031782052840	2021-04-25 18:01:57.433724	2021-04-25 18:01:57.89432	00:00:00.46...
15	287432	214031786719788	2021-04-25 18:08:43.047892	2021-04-25 18:13:57.498019	00:05:14.45...
16	287433	214031787073418	2021-04-25 18:20:47.050182	2021-04-25 18:20:47.515546	00:00:00.46...
17	287434	214031830682727	2021-04-25 18:02:00.185391	2021-04-25 18:02:14.739673	00:00:14.55...
18	287435	214032587015494	2021-04-25 18:15:04.655283	2021-04-25 18:15:19.231492	00:00:14.57...
19	287436	214032685056610	2021-04-25 18:10:00.65468	2021-04-25 18:10:01.155893	00:00:00.50...
20	287437	214032730007945	2021-04-25 18:02:49.924491	2021-04-25 18:08:03.87738	00:05:13.95...
21	287438	214032730192602	2021-04-25 18:03:15.610527	2021-04-25 18:18:55.690531	00:15:40.08...
22	287439	214032785062826	2021-04-25 18:16:25.994542	2021-04-25 18:16:26.458647	00:00:00.46...
23	287440	214032786671856	2021-04-25 18:13:44.963005	2021-04-25 18:15:05.452572	00:01:20.48...
24	287441	214032830348713	2021-04-25 18:18:46.713104	2021-04-25 18:18:46.713104	00:00:00
25	287442	214032885269863	2021-04-25 18:09:45.959492	2021-04-25 18:09:46.423086	00:00:00.46...
26	287443	214032887225685	2021-04-25 18:14:59.427088	2021-04-25 18:14:59.889674	00:00:00.46...
27	287444	214033574041119	2021-04-25 18:19:50.210399	2021-04-25 18:19:50.672144	00:00:00.46...

Figura 4.16 Tabla de datos procesados.

Estas operaciones se repiten para cada una de las capturas realizadas, almacenando los datos obtenidos para su análisis.

Desde la base de datos se exporta la información a *Microsoft Excel* donde se hace uso de las herramientas de tablas y gráficos dinámicos para mostrar los resultados más representativos fácilmente.

Los datos de partida contienen los IMSIs únicos detectados, primera y última aparición diaria y duración. Contando el número de identificadores detectados cada día es posible conocer el número de visitas diarias, sin tener en cuenta si son visitantes nuevos u antiguos.

Es posible calcular la diferencia del total de identificadores detectados respecto al número de identificadores no repetidos, obteniendo así el porcentaje de nuevos visitantes respecto a las visitas reiteradas.

Puesto que se tienen datos del tiempo que está cada dispositivo en la zona, se puede observar la distribución del tiempo de visita.

El conjunto de resultados se muestra en la página principal del archivo *Excel*, en una llamada *Dashboard* o tablero, que permite modificar las propiedades de las gráficas como fecha o duración (Figura 4.17).

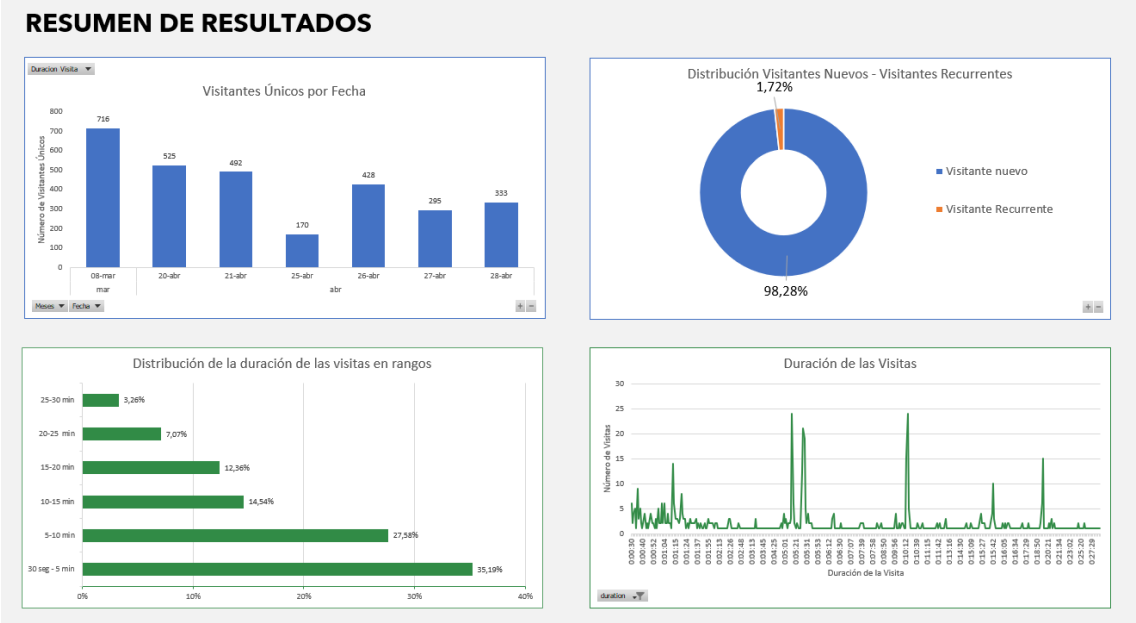

Figura 4.17 *Dashboard* de resultados.

La gráfica superior izquierda representa el número de visitantes únicos en función del día (Figura 4.18) siendo posible también ver el recuento mensual y anual (Figura 4.19) en el caso de una aplicación real.

Se detectan un total de 2959 dispositivos a lo largo de los 7 días de duración del ensayo, obteniendo el máximo el lunes 8 de marzo y el mínimo el domingo 25 de abril, al ser un día no laborable.

Figura 4.18 Visitantes únicos diarios.

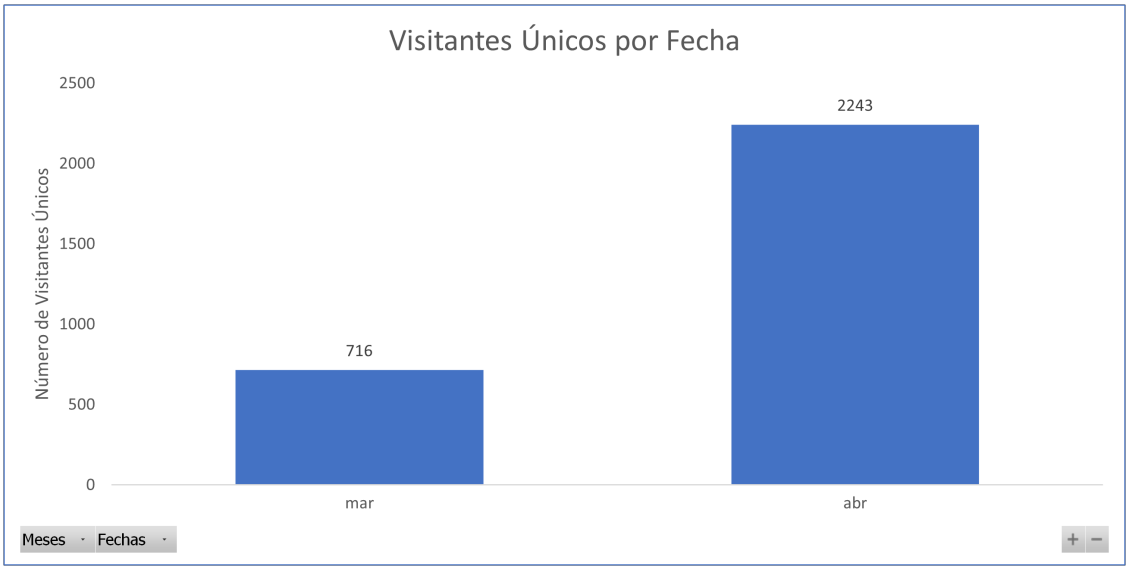

Figura 4.19 Visitantes únicos mensuales.

Respecto a la frecuencia de acceso, 2851 de las visitas son nuevas, 43 aparecen durante 2 días, 6 durante 3 días y únicamente 1 se repite durante 4 días. De esta manera, tal y como muestra la Figura 4.20, el 98.28 % de las visitas detectadas son nuevas.

Figura 4.20 Periodicidad de acceso.

Con respecto a los valores de duración, en la Figura 4.21 se observa un gran número de lecturas de duración 00:00:00. Este valor quiere decir que la primera captura y la última son la misma, el dispositivo solo ha sido captado por el receptor una vez.

Figura 4.21 Duración del conjunto completo de capturas.

Si el prototipo se implementara en un área comercial, las visitas que solo han sido detectadas un instante no constarían como clientes reales. Pueden deberse a vehículos o viandantes que pasan rápidamente por la zona.

Por no ser datos representativos de estancia, se decide eliminar todas las lecturas de duración 0, formando el histograma visible en la Figura 4.22.

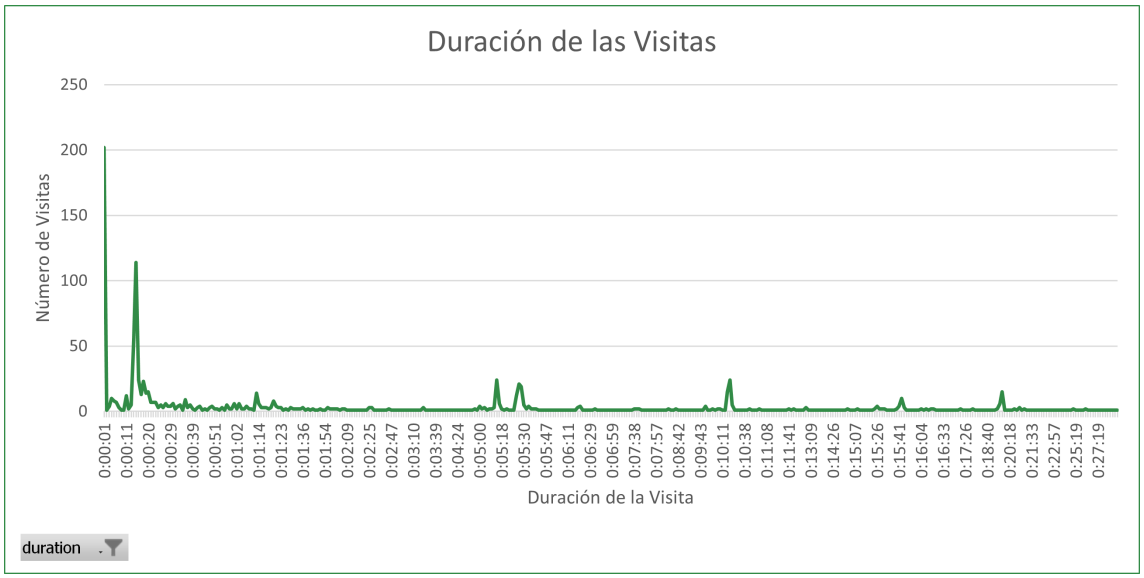

Figura 4.22 Duración de las visitas.

De igual manera, sigue habiendo valores atípicos en las capturas con duraciones de hasta 20 segundos. Si el receptor tomara medidas durante 12 horas en un centro comercial, sería lógico descartar aquellas inferiores de entre 5 y 10 minutos.

Puesto que el rango utilizado es considerablemente inferior (30 minutos), se decide eliminar aquellos identificadores cuya diferencia entre última y primera detección no supere los 30 segundos, obteniendo así una distribución más acertada y realista del tiempo de estancia de los dispositivos detectados (Figura 4.23).

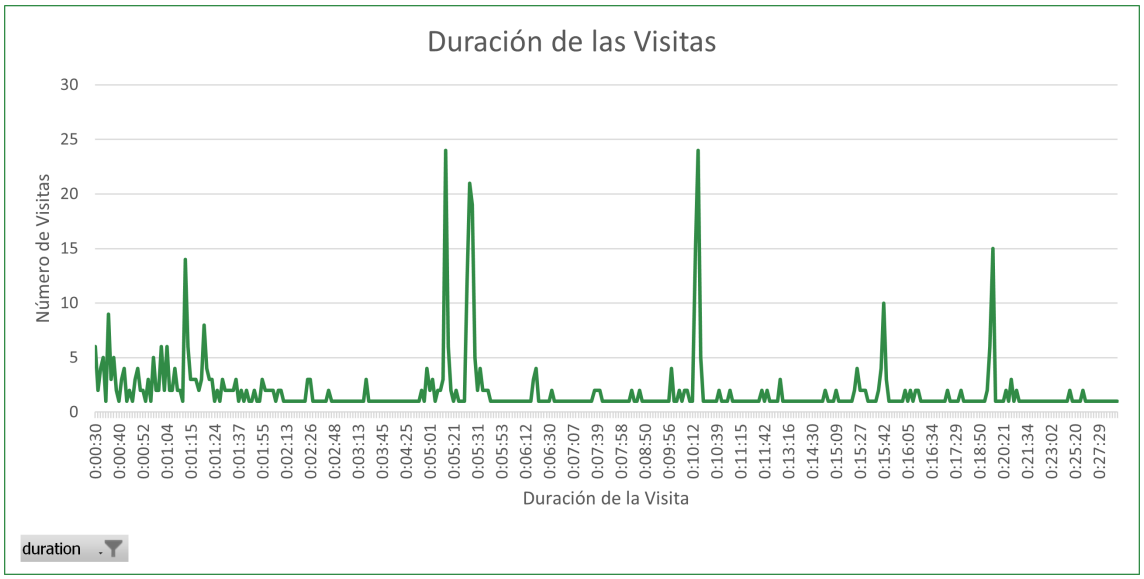

Figura 4.23 Duración de las visitas representativas.

En el caso de disponer de un mayor intervalo de tiempo, una estadística interesante es la distribución de visitas en rangos temporales inferiores, en este caso de 5 en 5 minutos. Para la Figura 4.24 se excluyen las mismas medidas que en la Figura 4.23, quedando definido el primer intervalo por las mediciones de duración entre 30 segundos y 5 minutos.

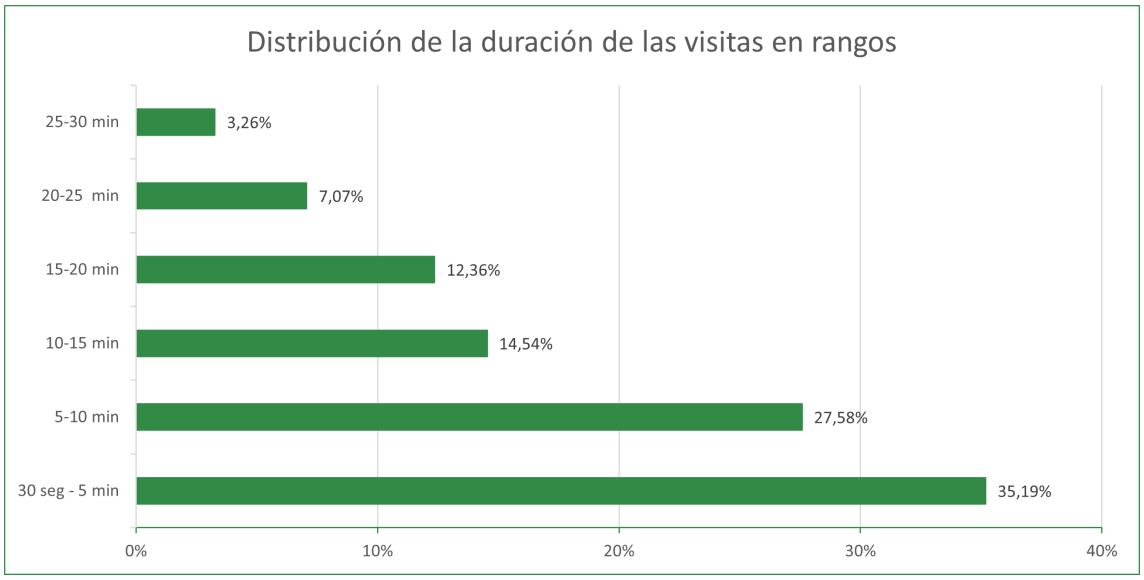

Figura 4.24 Distribución de la duración en rangos.

Se observa que la mayoría de usuarios (62.77 %) pasa menos de 10 minutos en la zona, pudiendo estar de paso o haciendo compras rápidas. En una aplicación mayor, podría utilizarse esta herramienta para comprobar la duración media de las visitas y las horas más concurridas de un establecimiento.

Además, permitiría desestimar con facilidad aquellas personas que no son potenciales clientes sino residentes de la zona o trabajadores, ya que su identificador se repetiría más que la media y pertenecerían al rango que más tiempo permanece en el área.

Por último, en la Figura 4.25 se recoge el número real de visitantes únicos diarios, según la duración mínima definida anteriormente. El número resultante es de 742 individuos, un 25.08 % del total medido sin filtros.

Figura 4.25 Visitantes únicos diarios con duración de la visita mínima.

5 Conclusiones y desarrollo futuro

Tras llevar a cabo el estudio sobre las diferentes tecnologías de conteo de personas y desarrollar el prototipo de receptor de IMSI, se establecen las conclusiones que se detallan a continuación, así como posibles líneas de desarrollo para una futura mejora del sistema.

- El IMSI como identificador de personas únicas: La generalización social del teléfono móvil, junto a su facilidad de obtención, invariabilidad y posibilidad de encriptarlo para mantener la seguridad del usuario hacen de este distintivo una opción ideal para el objetivo del trabajo. En comparación con las otras tecnologías estudiadas es mucho más accesible y extendido que la dirección MAC y permite reidentificación, al contrario que el estado del arte actual de la visión artificial.

- Uso de la tecnología SDR como receptor: El hardware utilizado es una opción de implementación de bajo precio y en el presente TFG se acredita su viabilidad para el conteo y reidentificación de personas. Sin embargo, se aprecian dos principales inconvenientes en su uso: por un lado, para cubrir por completo el área deseada es necesario un receptor por cada estación base que dé cobertura a la zona. Por otro lado está el hecho de que el hardware elegido no tenga capacidad suficiente para cubrir el rango de frecuencias completo de la red de telefonía.

- Precisión del sistema: Se trata de la principal limitación encontrada, ya que el área de captura no depende del dispositivo, sino de la operadora. No es posible asegurar que la precisión del conteo sea del 100 %, ya sea porque no todos los clientes dispongan de un teléfono móvil en el momento o, principalmente, porque las estaciones base no cubran con exactitud la zona de interés. Este factor se puede mitigar solicitando la información actualizada a las operadoras de interés.

- Procesamiento de grandes cantidades de datos: Durante las pruebas realizadas sobre el prototipo se obtuvieron alrededor de 2500 paquetes por minuto. Esto implica cientos de miles de datos a filtrar y procesar que, sin las herramientas adecuadas, ralentizarían el proceso por la gran carga computacional. La implementación de una base de datos supone una solución sencilla, que agiliza el acceso e introducción de datos, permite compartirlos y elimina las posibles limitaciones de espacio.

- Potencial de implementación real: La principal ventaja del sistema propuesto es el bajo precio y la facilidad de instalación y obtención de resultados. La necesidad de varios receptores no

supone una gran diferencia de inversión a gran escala. Además, no es necesario que dichos receptores estén conectados a un servidor central, sino que el software es configurable en pequeñas placas base que recogerían y enviarían los datos secuencialmente.

La limitación de precisión hace que no sea la opción ideal como tecnología de conteo principal. No obstante, si ya estuviera implementado un método alternativo más preciso, como pudiera ser un algoritmo de visión artificial, sería de interés la integración conjunta de ambos sistemas, añadiendo datos de reidentificación con el receptor IMSI y aumentando la exactitud a partir de los datos fiables del algoritmo.

- Propuestas de desarrollo futuro: Entre las mejoras implementables se encuentra la utilización de un equipo hardware más potente, que cubra todo el espectro radioeléctrico de telefonía y que permita la recepción de varios canales simultáneamente, reduciendo así el número de dispositivos necesarios.

  Por otro lado, hacer uso del identificador temporal TMSI para obtener medidas más precisas de la duración de las visitas, ya que es el dato más intercambiado entre el dispositivo móvil y la estación base.

  Por último, encontrar una solución equivalente para la tecnología 5G, que será la más extendida en el futuro cercano y utiliza un identificador distinto al IMSI.

Índice de Figuras

2.1 Plataforma de Análisis de información y generación de reportes [16] 4
2.2 Vector de Soporte en 2D [20] 6
2.3 Relación RSSI y Distancia (m) para 3 modelos de receptores diferentes [28] 10
2.4 Funcionamiento IMSI-Catcher Activo [31] 14

3.1 Emplazamiento estaciones base [33] 18
3.2 Arquitectura de las redes GSM, UMTS y LTE [34] 19
3.3 Bandas de frecuencias por operador [37] 21
3.4 Fases generales del protocolo AKA [40] 24

4.1 Hardware utilizado para el prototipo (Nooelec NESDR Smartee XTR) 27
4.2 Puesta en marcha del dispositivo 28
4.3 Recepción de señal de radiofrecuencia 29
4.4 Configuración del receptor de señales de telefonía 29
4.5 Búsqueda de estaciones base cercanas 30
4.6 Mapa estaciones cercanas a la Escuela según el Ministerio de Asuntos Económicos [51] 31
4.7 Desglose estación Vodafone cercana a la Escuela según el Ministerio de Asuntos Económicos [51] 32
4.8 Mapa estaciones cercanas a la Escuela según OpenCell Id [49] 32
4.9 Mapa estaciones cercanas a la Escuela según CellMapper [50] 33
4.10 Ventana control de la frecuencia de captura 34
4.11 Salida de la terminal al capturar señales 35
4.12 Salida del script de Python desarrollado para encontrar IMSIs únicos 35
4.13 Tráfico capturado en Wireshark con filtros de IMSI 36
4.14 Modo transmisor y receptor de la Diferencia de Tiempo de Llegada [53] 38
4.15 Tabla de datos sin procesar 40
4.16 Tabla de datos procesados 41
4.17 Dashboard de resultados 42
4.18 Visitantes únicos diarios 43
4.19 Visitantes únicos mensuales 43
4.20 Periodicidad de acceso 44
4.21 Duración del conjunto completo de capturas 44
4.22 Duración de las visitas 45
4.23 Duración de las visitas representativas 45

4.24 Distribución de la duración en rangos 46
4.25 Visitantes únicos diarios con duración de la visita mínima 47

Índice de Tablas

2.1 Comparación de Medidas. Total de personas: 6074 8
2.2 Evaluación de las métricas para cada algoritmo 8
2.3 Resumen Métodos de Identificación y Conteo 15

Bibliografía

[1] D. Y. Chen and K. Y. Lin, "A novel viewer counter for digital billboards," *IIH-MSP 2009 - 2009 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 653–656, 2009. [Online]. Available: https://ieeexplore.ieee.org/document/5337426

[2] X. Liu, P. H. Tu, J. Rittscher, A. Perera, and N. Krahnstoever, "Detecting and counting people in surveillance applications," *IEEE International Conference on Advanced Video and Signal Based Surveillance - Proceedings of AVSS 2005*, vol. 2005, pp. 306–311, 2005. [Online]. Available: https://ieeexplore.ieee.org/document/1577286

[3] "The 6 most important web metrics to track for your business website," (Last accessed 05/04/2021). [Online]. Available: https://articles.bplans.com/the-6-most-important-web-metrics-to-track-for-your-business-website/

[4] F. Nicasio, "The ultimate guide to foot traffic and people counting," 11 2019, (Last accessed 06/04/2021). [Online]. Available: https://blog.getdor.com/2019/11/11/foot-traffic-people-counting/

[5] C. Samsing, "Las métricas de retención de clientes que realmente importan," 9 2020, (Last accessed 07/04/2021). [Online]. Available: https://blog.hubspot.es/service/metricas-retencion-clientes

[6] V. Prabakaran, A. Arthanariee, and M. Sivakumar, "Crowd safety: A real time system for counting people," *INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING*, vol. 1, 2011.

[7] S. Velipasalar, Y. L. Tian, and A. Hampapur, "Automatic counting of interacting people by using a single uncalibrated camera," *2006 IEEE International Conference on Multimedia and Expo, ICME 2006 - Proceedings*, vol. 2006, 2006.

[8] H. Cetinkaya and M. Akcay, "People counting at campuses," *Procedia-Social and Behavioral Sciences*, vol. 182, pp. 732–736, 2015. [Online]. Available: www.sciencedirect.com

[9] I. Haritaoglu, D. Harwood, and L. S. Davis, "Hydra: Multiple people detection and tracking using silhouettes," *Proceedings - 2nd IEEE International Workshop on Visual Surveillance, VS 1999*, pp. 6–13, 1999. [Online]. Available: https://ieeexplore.ieee.org/document/780263

[10] S. Yu, X. Chen, W. Sun, and D. Xie, "A robust method for detecting and counting people," *ICALIP 2008 - 2008 International Conference on Audio, Language and Image Processing, Proceedings*, pp. 1545–1549, 2008. [Online]. Available: https://ieeexplore.ieee.org/document/4590257

[11] A. K. Mahamad, S. Saon, H. Hashim, M. A. Ahmadon, and S. Yamaguchi, "Cloud-based people counter," *Bulletin of Electrical Engineering and Informatics*, vol. 9, 2020.

[12] Proconsi, "Sistema de conteo de personas en tiempo real - smartcounter," (Last accessed 25/04/2021). [Online]. Available: https://www.proconsi.com/sistema-de-conteo-de-personas-en-tiempo-real-smartcounter

[13] Ismena, "People counting – isolutions," (Last accessed 25/04/2021). [Online]. Available: https://www.ismena.com/people-counting/

[14] Cadlan, "Soluciones para el sector retail: Tecnología aplicada a empresas retail," (Last accessed 25/04/2021). [Online]. Available: https://www.cadlan.com/verticales-retail/

[15] F. Analytics, "Insights | flame analytics," (Last accessed 25/04/2021). [Online]. Available: https://flameanalytics.com/insights/

[16] Fevox, "Conteo de personas - sensores con software avanzado," (Last accessed 25/04/2021). [Online]. Available: https://www.fevox.co/solution/conteo-de-personas/

[17] Centum-rt, "Lifeseeker," (Last accessed 25/04/2021). [Online]. Available: http://www.centum-rt.com/en/lifeseeker/

[18] C. Raghavachari, V. Aparna, S. Chithira, and V. Balasubramanian, "A comparative study of vision based human detection techniques in people counting applications," *Procedia Computer Science*, vol. 58, pp. 461–469, 1 2015. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1877050915021754

[19] M. Padmashini, R. Manjusha, and L. Parameswaran, "Vision based algorithm for people counting using deep learning," *International Journal of Engineering & Technology*, vol. 7, p. 74, 7 2018. [Online]. Available: https://www.sciencepubco.com/index.php/ijet/article/view/14942

[20] "Máquinas de vectores de soporte (svm) - iartificial.net," (Last accessed 05/05/2021). [Online]. Available: https://www.iartificial.net/maquinas-de-vectores-de-soporte-svm/

[21] M. Pietikäinen, "Local binary patterns," *Scholarpedia*, vol. 5, p. 9775, 2010. [Online]. Available: http://http://www.scholarpedia.org/article/Local_Binary_Patterns

[22] G. Learning, "Adaboost algorithm: Boosting algorithm in machine learning," 5 2020, (Last accessed 10/05/2021). [Online]. Available: https://www.mygreatlearning.com/blog/adaboost-algorithm/

[23] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, and M. Andreetto, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," 2017. [Online]. Available: https://arxiv.org/abs/1704.04861v1

[24] Z. Cheng, X. Zhu, and S. Gong, "Face re-identification challenge: Are face recognition models good enough?" *Pattern Recognition*, vol. 107, p. 107422, 11 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0031320320302259

[25] Y. Zhou, "Deep learning based people detection, tracking and re-identification in intelligent video surveillance system," *2020 International Conference on Computing and Data Science (CDS)*, pp. 443–447, 8 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9275961/

[26] I. Arhipova, G. Vitols, and I. Meirane, "Long period re-identification approach to improving the quality of education: A preliminary study," *Advances in Intelligent Systems and Computing*, vol. 1130 AISC, pp. 157–168, 3 2020. [Online]. Available: https://doi.org/10.1007/978-3-030-39442-4_14

[27] A. Bensky, *Wireless Positioning Technologies and Applications*. USA: Artech House, Inc., 2007.

[28] D. Oosterlinck, D. F. Benoit, P. Baecke, and N. V. de Weghe, "Bluetooth tracking of humans in an indoor environment: An application to shopping mall visits," *Applied Geography*, vol. 78, pp. 55–65, 1 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0143622816307330

[29] N. Abedi, A. Bhaskar, E. Chung, and M. Miska, "Assessment of antenna characteristic effects on pedestrian and cyclists travel-time estimation based on bluetooth and wifi mac addresses," *Transportation Research Part C: Emerging Technologies*, vol. 60, pp. 124–141, 11 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0968090X15003113

[30] P. B. Copet, G. Marchetto, R. Sisto, and L. Costa, "Formal verification of lte-umts and lte-lte handover procedures," *Computer Standards and Interfaces*, vol. 50, pp. 92–106, 2 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S092054891630071X

[31] A. Lilly, "Imsi catchers: hacking mobile communications," *Network Security*, vol. 2017, pp. 5–7, 2 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1353485817300144

[32] M. Naarttijärvi, "Swedish police implementation of imsi-catchers in a european law perspective," *Computer Law and Security Review*, vol. 32, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364916301200

[33] H. Moya, *Comunicaciones moviles: sistemas GSM, UMTS y LTE*. RA-MA Editorial, 2014. [Online]. Available: https://elibro--net.us.debiblio.com/es/ereader/bibliotecaus/106423

[34] "¿qué elementos componen una red móvil? | temas tecnologicos de interes," (Last accessed 24/05/2021). [Online]. Available: https://www.temastecnologicos.com/redes-moviles/elementos/

[35] "Ministerio de asuntos económicos y transformación digital - espectro radioeléctrico," (Last accessed 24/05/2021). [Online]. Available: https://avancedigital.mineco.gob.es/espectro/Paginas/index.aspx

[36] "*Boletín Oficial del Estado*, 259, de 27 de octubre de 2017, 103115 a 103478," (Last accessed 24/05/2021). [Online]. Available: https://www.boe.es/eli/es/o/2017/10/25/etu1033

[37] "Bandas del 5g, 4g, 3g y 2g en españa: frecuencias telefonía móvil de cada operador – repetidores móviles," (Last accessed 24/05/2021). [Online]. Available: https://blog.repetidoresmoviles.com/bandas-del-5g-4g-3g-y-2g-en-espana-frecuencias-telefonia-movil-de-cada-operador/

[38] V. N. Payal, "Evaluation of authentication and ciphering algorithms in gsm," *International Journal of Computer Science and Mobile Computing*, vol. 3, pp. 379–392, 7 2014. [Online]. Available: https://www.ijcsmc.com/docs/papers/July2014/V3I7201487.pdf

[39] J.-K. Tsay and S. F. Mjølsnes, "A vulnerability in the umts and lte authentication and key agreement protocols," *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, vol. 7531, pp. 65–76, 2012. [Online]. Available: https://uia.brage.unit.no/uia-xmlui/bitstream/handle/11250/137418/master_ikt_2001_dohmen.pdf?sequence=1&isAllowed=y

[40] A. Rellstab, "Formalizing and verifying generations of aka protocols," 10 2019, (Last accessed 25/05/2021). [Online]. Available: https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/information-security-group-dam/research/software/ma-19-rellstab-AKA.pdf

[41] V. K. Garg, *Fourth Generation Systems and New Wireless Technologies*. Elsevier, 1 2007. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780123735805500570

[42] "Rtl-sdr," (Last accessed 26/05/2021). [Online]. Available: https://www.rtl-sdr.com/about-rtl-sdr/

[43] "Nooelec - nooelec nesdr smartee xtr bundle - nesdr rtl-sdr receivers - sdr receivers - software defined radio," (Last accessed 26/05/2021). [Online]. Available: https://www.nooelec.com/store/sdr/sdr-receivers/nesdr/nesdr-smartee-xtr.html

[44] "Hackrf," (Last accessed 26/05/2021). [Online]. Available: https://greatscottgadgets.com/hackrf/

[45] "Gnu radio - the free & open source radio ecosystem · gnu radio," (Last accessed 26/05/2021). [Online]. Available: https://www.gnuradio.org/

[46] P. Krysik, "gr-gsm," (Last accessed 26/05/2021). [Online]. Available: https://github.com/ptrkrysik/gr-gsm

[47] "Wireshark," (Last accessed 26/05/2021). [Online]. Available: https://www.wireshark.org/

[48] "Postgresql," (Last accessed 26/05/2021). [Online]. Available: https://www.postgresql.org/

[49] U. Labs, "Opencellid - largest open database of cell towers & geolocation," (Last accessed 01/06/2021). [Online]. Available: https://www.opencellid.org/#zoom=18&lat=37.411542&lon=-6.000168

[50] "Cellular coverage and tower map," (Last accessed 01/06/2021). [Online]. Available: https://www.cellmapper.net/map

[51] G. de España. Ministerio de Economía y Empresa, "Niveles de exposición," (Last accessed 01/06/2021). [Online]. Available: https://geoportal.minetur.gob.es/VCTEL/vcne.do

[52] J. Figueiras, S. Frattasi, and J. Figueiras, "Fundamentals of positioning," in *Mobile Positioning and Tracking: From Conventional to Cooperative Techniques*. John Wiley and Sons, 5 2010, pp. 61–90. [Online]. Available: https://ebookcentral.proquest.com/lib/uses/detail.action?docID=530039

[53] K. Sithamparanathan and A. Giorgetti, *Cognitive radio techniques : spectrum sensing,*

interference mitigation, and localization. Artech House, 2012. [Online]. Available: https://ebookcentral--proquest--com.us.debiblio.com/lib/uses/reader.action?docID=1118872