UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Análisis de la Seguridad y Proceso de la Auditoría de Señales

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

Autor: Víctor Aguado de Astorza

Tutor: Román García García

Curso 2016-2017

Resum

Aquest treball ha estat realitzat per establir una metodologia de l'anàlisi de les comunicacions de ràdio de diferents protocols. Així mateix s'han identificat les vulnerabilitats conegudes d'alguns d'aquests, sent possible en algun dels casos aprofitar-les. En aquest treball no s'han tingut en compte tecnologies com Bluetooth, NFC o Wi-Fi, pel fet que ja hi ha molta bibliografia sobre la seguretat d'aquestes.

Paraules clau: RF, Radio, Frecuencia, Modulació, Seguridad, SDR, TETRA, Inhibidor

Resumen

Este trabajo ha sido realizado para establecer una metodología del análisis de las comunicaciones de radio de diferentes protocolos. Así mismo se han identificado las vulnerabilidades conocidas de algunos de estos, siendo posible en alguno de los casos aprovechar estas. En este trabajo no se han tenido en cuenta tecnologías como Bluetooth, NFC o Wi-Fi, debido a que ya existe mucha bibliografía sobre la seguridad de estas.

Palabras clave: RF, Radio, Frecuencia, Modulación, Seguridad, SDR, TETRA, Inhibidor

Abstract

This work has been done to establish a methodology for the analysis of radio communications of different protocols. Also the known vulnerabilities of some of these have been identified, being possible in some of the cases to exploit them. In this work, technologies such as Bluetooth, NFC or Wi-Fi have not been taken into account, because there is already a lot of literature on the security of these.

Key words: RF, Radio, Frequency, Modulation, Security, SDR, TETRA, Jammer

Índice general

Índice de figuras

CAPÍTULO 1
Introducción

1.1 Motivación

La motivación principal de este proyecto parte de la curiosidad por la seguridad que proporcionan tecnologías como el RFID y como estas son usadas a diario en la electrónica de consumo, siendo que en muchos casos no se hace uso de ninguna medida de seguridad por parte de los fabricantes.

Se ha tratado de identificar el impacto producido por un uso ilícito de estas tecnologías y como puden afectar a los usuarios. Así mismo se ha tratado comprobar cual es el impacto real que podrían ocasionar las vulnerabilidades de estos sistemas de comunicación y sus protocolos en la sociedad actual. Además, no se hace uso de estas tecnologías únicamente en la electrónica de consumo, sino también en entornos industrializados y profesionales o gubernamentales, con lo que ello implica.

1.2 Objetivos

El objetivo primario de este proyecto consiste en el desarrollo de una metodología para el análisis de la seguridad de los sistemas de radiofrecuencia usados en entornos industriales y domésticos. Dentro de esta metodología se ha descartado el análisis de la seguridad tecnologías de uso cotidiano como pudieran ser Bluetooth o Wifi. Esto es así debido a que de estos protocolos ya existe documentación y metodologías para analizar su seguridad.

Para ello se tendrán en cuenta los siguientes objetivos secundarios:

- Identificación de las frecuencias más usadas para comunicaciones y transmisión de datos, así como los cifrados o protocolos usados.
- Búsqueda y presupuestado del equipamiento básico necesario para realizar una auditoría de las señales de radio usadas.
- Configuración del entorno y materiales para su uso.
- Establecer los pasos a seguir, de forma similar a la metodología OSSTMM.
- Interceptación de las transmisiones y obtención de los datos.

1.3 Estructura de la memoria

La estructura de la obra esta realizada de la siguiente manera:

- **Introducción:** El capítulo inicial de la obra. Se compone de las motivaciones para la realizacón del proyecto, los objetivos y la estructura de esta con una breve descripción.
- **Estado del arte:** Se presentan los estudios realizados hasta el momento sobre la temática, así mismo se presentan diversas tecnologias y problematicas identificadas durante el proceso de la realización de la obra.
- **Procedimientos a seguir:** Metodología realizada para llevar a cabo los análisis de diversas tecnologías seleccionadas a los largo del estado del arte.
- **Conclusión:** Se concluye con los resultados y esperiencias adquiridas.
- **Bibliografía:** Referencias relevantes usadas en el proceso de realización del proyecto.
- **Apéndices:** Información adicional relacionada con el proyecto.

CAPÍTULO 2
Estado del arte

El caso más próximo a una metodología de señales de radiofrecuencia que podemos encontrar es OSSTMM, pero esta es demasiado genérica y se centra más en las telecomunicaciones que en el análisis de los métodos de comunicación.

El caso más común que se puede encontrar, en lo que se refiere a vulnerabilidades de los sistemas de radiofrecuencia, es el uso de inhibidores de frecuencia. Esto consiste en la emisión de interferencias para uno o varios rangos de frecuencias concretos, esta técnica es conocida como *jamming* y es usada alrededor de todo el mundo, por ejemplo, en edificios públicos y oficiales. A parte de los problemas de comunicaciones en redes móviles que esto puede ocasionar (como la falta de cobertura en los terminales), también afecta a otros sistemas de radiofrecuencia que hagan uso de las frecuencias en las que el inhibidor está emitiendo, por ejemplo sistemas de apertura de vehículos, transmisiones de *walkie-talkie*...

Por ello, hay que tener en cuenta la cantidad de productos que realizan envíos de señales o que son susceptibles de sufrir interferencias a causa de estas. Sistemas de localización de ganado, seguimiento de activos, tele-pagos en autopistas (Via-T) , monitores de bebé, control de acuíferos, teclados y ratones inalámbricos, comunicaciones de servicios de seguridad, alarmas... Hay muchos dispositivos susceptibles de ataques por radiofrecuencia, ya sea generando interferencias, interceptando las transmisiones o realizando transmisiones ilícitas.

Todo lo comentado anteriormente no suele ser controlado y se considera seguro, pero en muchos casos esto es simplemente a causa de que no se tiene en cuenta que esto pueda ser susceptible de tener un fallo de seguridad. En algunos casos, estas señales se pueden interceptar con relativa facilidad y sin necesidad de equipamiento especializado.

El equipamiento necesario es sencillo de conseguir y no tiene un precio que se pueda considerar elevado. En el caso de una auditoría lógica, el técnico se valdría de escáneres de frecuencia para identificar la frecuencia exacta, así como de analizadores para determinar el tipo de tecnología del cual podría tratarse.

De forma adicional al hardware que se considera más profesional, se pueden encontrar dispositivos que pueden ofrecer resultados similares por apenas unos 20 euros. Básicamente estos dispositivos son receptores DVB-T que pueden ser usados como Software Defined Radio (SDR en adelante). Estos aparatos, en la mayoría de los casos, permiten la

recepción de señales de radio en frecuencias que van desde lo 30MHz a los 1,7 GHz.

En caso de querer transmitir, sería necesario adquirir un equipamiento con un coste mayor. Aun así se puede considerar relativamente barato. El precio de estos equipos es aproximadamente de unos 350 euros, para un equipamiento básico.

Al coste inicial de este equipamiento habría que añadir el coste relativo a las antenas para las diferentes frecuencias a sintonizar, el precio de estas se encuentra entre los 30 y 90 euros. Otro equipamiento secundario como pudieran ser filtro y amplificadores. Pero esto en la mayoría de los casos no es indispensable.

Del mismo modo, se puede encontrar una gran cantidad de información al respecto del uso de estos dispositivos, con ejemplos de uso, tutoriales sobre su configuración y documentación sobre el funcionamiento interno. En lo que se refiere a datos sobre los diferentes protocolos usados para las transmisiones también se puede encontrar información fácilmente, no siempre al nivel más adecuado, pero el suficiente para entender cómo funcionan.

Hasta el momento hay pruebas de concepto (PoC) sobre vulnerabilidades relacionadas con estos sistemas. Incluso se ha conseguido obtener datos de equipos aislados de la red, es decir, sin ningún tipo de conexión a una red de datos por Wifi, Bluetooth o cable de red. Para ello se usó un malware que se instalaba en el equipo a través de, por ejemplo, una unidad flash y por medio de un análisis de las señales de radio emitidas por el equipo se podían obtener las diferentes pulsaciones del teclado, es decir, un *keylogger*. Esta técnica recibe el nombre de Airhopper.

Así mismo otras pruebas han demostrado que con un hardware muy sencillo y barato, unos 37$, sistemas de cerradura electrónica controlados por radio en vehículos son explotables. Lo que significa que se podría abrir un vehículo sin tener que forzar físicamente su cerradura y en algunos casos incluso arrancar el motor.

2.1 Problemática

El principal problema de las tecnologías de las comunicaciones por radiofrecuencia radica en que más allá de WiFi, Bluetooth, o más recientemente, NFC, que son consideradas soluciones de uso cotidiano, el resto están relativamente olvidadas y apenas se les da visibilidad dentro del mercado. Esto implica que las medidas de seguridad que usan hayan quedado desfasadas o sean prácticamente inexistentes.

Si bien es cierto que hoy prácticamente cualquier dispositivo tiene su variante inalámbrica, la solución proporcionada suele ser propietaria y por ello se asume que es segura. Así mismo en el mercado actual se encuentran diferentes dispositivos de uso común que interactúan entre sí, formando lo que se conoce como Internet de las cosas, IoT por sus siglas en inglés (*Internet of Things*).Todos estos dispositivos se consideran seguros por definición o porqué los datos que envían/reciben son de ínfima relevancia. En este caso el mayor problema es que esta clase de tecnologías (ZigBee, SigFox, LoRa,...) están implantándose en entornos industriales donde sí que pueden transmitir datos de importancia, como pudieran ser datos sobre el estado de una red eléctrica o gestionen sistemas de cultivos.

2.2 Modulaciones

Antes de hablar sobre las tecnologías en sí, es necesario tener en cuenta las diferentes modulaciones que son usadas por estas. Las modulaciones que pueden considerarse básicas son FSK, ASK y BPSK, de estas surgen diferentes variaciones pero manteniendo siempre el mismo concepto básico de funcionamiento. Todas ellas consisten en la modulación de una señal digital con una portadora analógica.

2.2.1. Modulación FSK

La modulación FSK en la que tenemos una señal con los datos (Data - Figura 1) y una señal portadora (Carrier - Figura 1) la modulación resultante provoca que, en este caso por ser FSK, cuando el dato introducido representa un 0 la señal obtenida tiene una frecuencia menor.

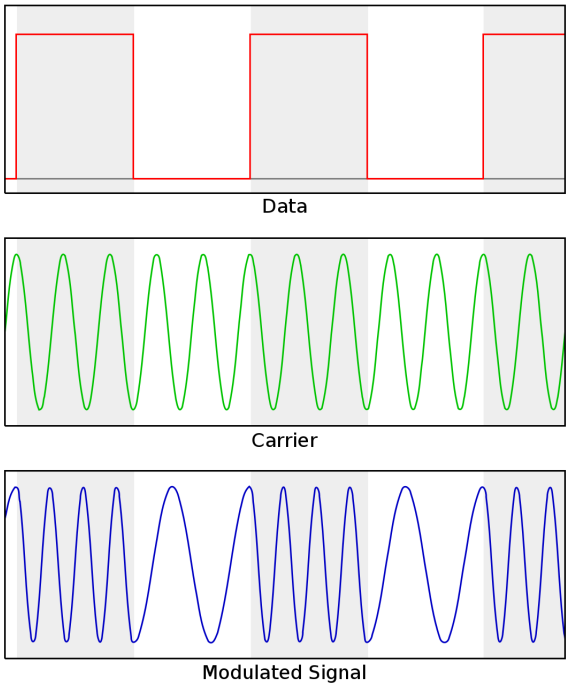

Figura 2.1: Modulación FSK

En el caso de esta modulación se asigna una frecuencia diferente a cada uno de los valores de la entrada de datos digital. Esta entrada solo puede tener dos estados, 1 y 0, por lo que se generan dos frecuencias una frecuencia alta (***F1***) asignada al estado 1 y otra baja (***F0***) asignada al estado 0. Estas frecuencias son asignadas en relación al centro de la frecuencia (***Fc***) de la portadora.

Para que la señal modulada resultante sea continua y no se produzcan cambios abruptos de frecuencia entre la frecuencia alta y baja, este se realiza mediante un VCO (*Voltage Controlled Oscillator*), el cual cambia la frecuencia en proporción al voltaje de la señal de entrada. En las siguientes figuras se observa la diferencia entre usar un VCO o hacer uso de dos osciladores.

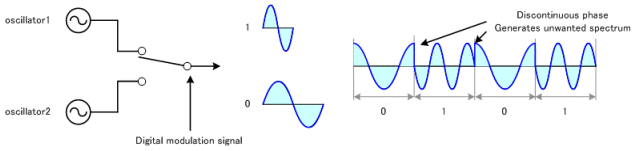

Figura 2.2: Modulación FSK con dos osciladores

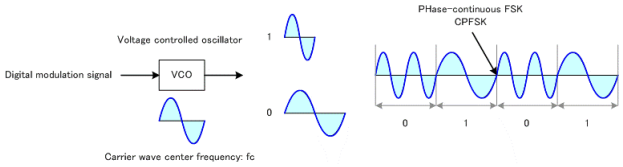

Figura 2.3: Modulación FSK con VCO

Para la obtención de los valores relativos a la frecuencia alta y mínima, así como a la frecuencia en cada momento temporal se hace uso de las siguientes funciones algebraicas.

$$F0(t) = Ac \times \cos\{2\pi\,(FC - \Lambda f)\,t\}$$

$$F1(t) = Ac \times \cos\{2\pi\,(FC - \Lambda f)\,t\}$$

Donde el parámetro Fc indica la frecuencia portadora, Ac la amplitud de la portadora y Λc el desplazamiento máximo de la frecuencia de la frecuencia.

La señal combinada puede ser descrita de la siguiente forma, teniendo en cuenta que los dos términos son ortogonales en el tiempo y nunca pueden ocurrir de forma simultánea.

$$S_{BFSK}(t) = A_{F1} \times \cos(2\pi \times F1 \times t) + A_{F0} \times \cos(2\pi \times F0 \times t)$$

2.2.2. Modulación ASK

En el caso de una modulación OOK (*On-Off Keyshift*) la señal modulada resultante sufre variaciones en su amplitud, esto ocurre únicamente cuando se modifican los valores de la señal digital. Es decir, dependiendo de si el valor introducido en ese instante de tiempo es un 1 o un 0 (*Data*) la señal resultante modificará (*Modulated Signal*) su amplitud.

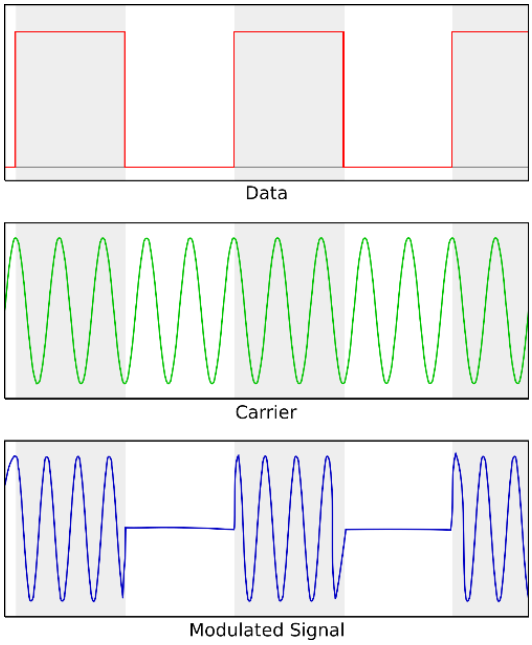

Figura 2.4: Modulación OOK, caso extremo de ASK

Este tipo de modulación es una variación llevada al extremo de la modulación ASK (*Amplitude Shift Keying*), de la cual existen dos tipos de detección (síncrona y asíncrona).

En la figura siguiente se observa cual es el diagrama base usado en la modulación.

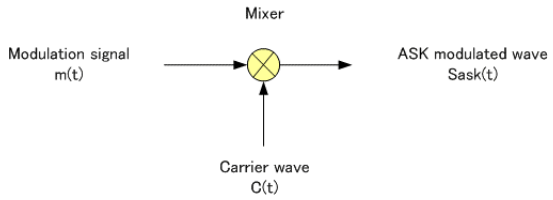

Figura 2.5: ASK con detección síncrona

La expresión algebraica correspondiente a la señal portadora $C(t)$ (*Carrier wave*) es la siguiente, donde A_c corresponde con la amplitud de la señal portadora (*carrier*) y F_c a la frecuencia de la señal portadora.

$$C(t) = A_c \times \cos(F_c 2\pi \times t)$$

El resultado de la señal modulada en ASK (*ASK modulated wave*, $S_{ask}(t)$) es la multiplicación de $m(t)$ (*Modulation signal*) expresado como la fórmula es el siguiente:

$$S_{ask}t = m(t) \times C(t) = m(t) \times A_c \times \cos(F_c \times 2\pi \times t)$$

En el caso de la modulación ASK con detección síncrona el proceso a seguir es el indicado en el diagrama siguiente:

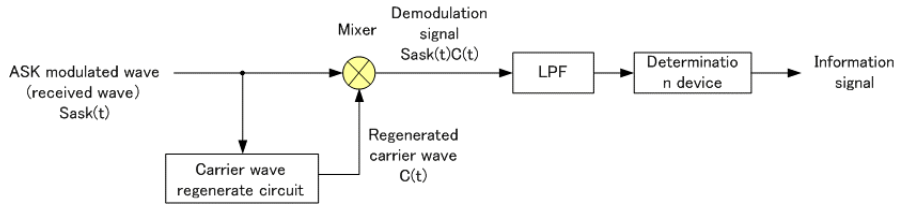

Figura 2.6: ASK con detección síncrona

En este sistema se añade un circuito regenerador de la señal portadora (*Carrier wave regenerate circuit*) así como un flitro por paso bajo (*Low Pass Filter*, LPF). El dispositivo de determinación (*Determination device*), determina el nivel de la señal resultante y obtiene la señal de información final a transmitir.

En términos algebraicos el regenerador de la señal se corresponde con la siguiente fórmula:

$$S_{ask}(t) \times C(t) = m(t) \times A_c \times \cos^2(F_c \times 2\pi \times t) = m(t) \times A_c \times \frac{1}{2} \times \{1 + \cos(4 \times \pi \times F_c \times t)\}$$

A causa de que el segundo término entre las llaves es algo que no se busca, la formula puede ser simplificada añadiendo únicamente el LPF:

$$\langle S_{ask}(t) \times C(t) \rangle_{LPF} = \frac{A_c}{2} \times m(t)$$

Si la detección es asíncrona la señal modulada en ASK es multiplicada por un cuadrado, tal como se puede observar en el diagrama mostrado en la siguiente figura.

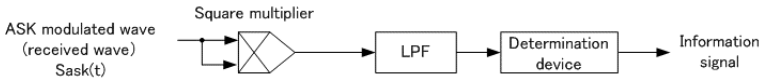

Figura 2.7: ASK con detección asíncrona

Los términos algebraicos que representan esta detección asíncrona son los siguientes:

$$S^2_{ask}(t) \times C(t) = m^2(t) \times A_c \cos^2(F_c \times 2\pi \times t) = m^2(t) \times A_c^2 \times \frac{1}{2} \times \{1 + \cos(4 \times \pi \times F_c \times t)\}$$

Del mismo modo que en la detección síncrona, el segundo término entre llaves es algo que no se requiere, por ello se aplica el LPF.

$$\langle S^2_{ask}(t) \times C(t) \rangle_{LPF} = \frac{A_c^2}{2} \times m^2(t)$$

2.2.3. Modulación PSK

PSK (*Phase Shift Keying*) es un tipo de modulación digital con un bajo índice de error. La fase de la onda portadora es modificada siendo asignada a un bit de los bits de la información a transmitir. Las variaciones de esta modulación son BPSK (*Binary Phase Shift*

Keying), QPSK (*Quadrature Phase Shift Keying*) y 8PSK.

Dado que la base de este tipo de modulaciones se puede considerar que es BPSK, el resto son ampliaciones de esta, se explicará únicamente esta.

En la modulación BPSK se usa un símbolo compuesto por un bit, para los niveles de la señal de entrada (1 y 0) se asignan los valores 1 y -1, ya que se trata de una señal dipolar NRZ (*Non Return to Zero*) y la fase de la señal portadora es asignada a 0 o π.

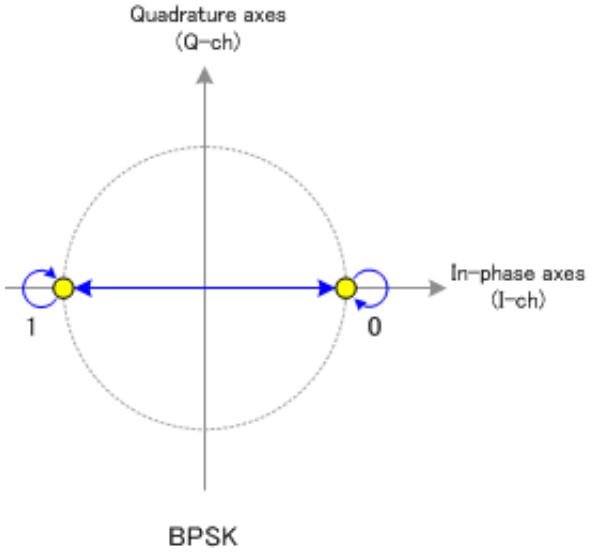

Figura 2.8: Constelación BPSK

Como se ha explicado previamente, en este tipo de modulación los valores de la señal de entrada digital (0 y 1) son convertidos en una señal NRZ dipolar. Esta señal y la portadora son multiplicadas entre sí.

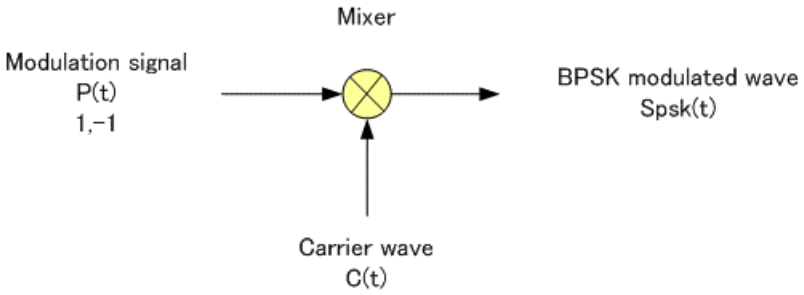

Figura 2.9: Diagrama de modulación BPSK

La fase de la señal portadora $C(t)$ es modificada proporcionalmente a la información de la señal de entrada. $C(t)$ es una onda sinusoidal con la siguiente forma, donde Φ_c es la fase de la portadora:

$$C(t) = A_c \times \cos(2\pi \times F_c \times t + \Phi_c)$$

Modifica la fase de la onda portadora entre 0 y 180 grados en relación los dos estados de la información introducida, dando como resultado la siguiente formula.

$$S_{psk} = A_c \times \cos\{2\pi \times F_c \times t + \Phi_c + \pi \times m(t)\}$$

Cuando la fase inicial de la portadora es $\Phi = 0$;

$$S_{psk} = A_c \times \cos\{\pi \times m(t)\} \times \cos(2\pi \times F_c \times t)$$

$P(t)$ puede tomar los valores 1 y -1 (*Modulation Signal* $P(t)$)

$$P(t) = \cos\{\pi \times m(t)\}$$

Esta es multiplicada por la señal portadora tal como se muestra en la figura previa. Por tanto la forma algebraica de los valores de la señal modulada es la siguiente.

$$S_{psk}(t) = P(t) \times C(t) = P(t) \times A_c \times \cos(2\pi \times F_c \times t)$$

Es decir, 1 bit de información puede ser expresado con 1 símbolo. Como se muestra en primera figura, la información se asigna a 0 y π con los valores 0 y 1 respectivamente. Dando como resultado su modulación algo similar a lo mostrado en las siguientes figuras.

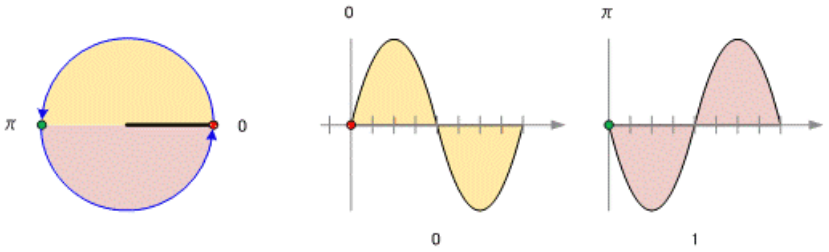

Figura 2.10: Ejemplo 1 BPSK

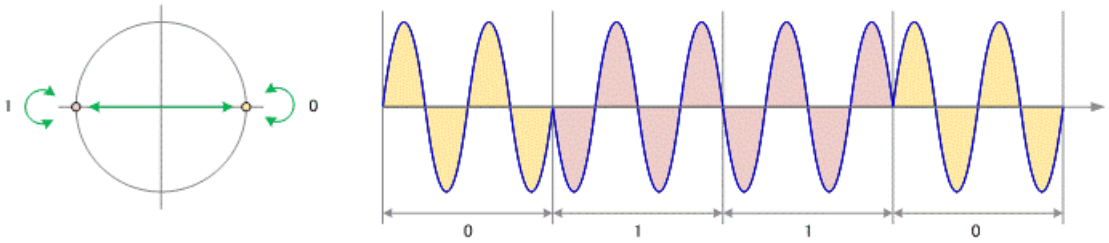

Figura 2.11: Ejemplo 2 BPSK

Este es un ejemplo de la modulación BPSK. Sobre esta pueden realizarse diversas variaciones. Por ejemplo, se puede aumentar la cantidad de símbolos en la modulación PSK, teniendo como resultado modulaciones QPSK o 8PSK.

2.3 Tecnologías comunes

En esta sección se abordarán algunas de las tecnologías más extendidas, incluyendo tanto de uso doméstico como uso industrial.

2.3.1. Telemandos

Sin llegar a ser una tecnología concreta como tal, su uso se encuentra tan extendido que han de ser mencionados para su posterior análisis. Son dispositivos de un coste relativamente bajo, usados habitualmente para la manipulación remota de puertas de garaje,

alarmas de vehículos... Consiste en la transmisión una señal de radio la cual es interpretada por el receptor.

La complejidad de estos dispositivos es diversas dependiendo del uso y el fabricante. En la mayoría de los casos se usa una modulación ASK, concretamente una variación de esta, OOK, pero también se pueden encontrar casos en los que se usan modulaciones 2FSK (variación de FSK) o incluso AM, como se verá más adelante. En lo que a las frecuencias usadas, es común el uso de las bandas 315Mhz, 433Mhz o 868Mhz, pero una vez más, dependiendo del fabricante se puede alejar de estos estándares.

La implementación más sencilla consiste en la transmisión de un mensaje o código, que identifica al dispositivo frente al receptor, el cuál no varía en el tiempo ni en el uso, es decir un código estático. Sistemas más complejos hacen uso de técnicas que consisten en variar este mensaje. Entre esto, se encuentran los conocidos como *rolling codes*, consiste en variar el mensaje enviado en cada emisión. Para que el receptor reconozca el código recibido como legítimo se utilizan diversas técnicas, entre ellas comprobar si lo recibido se encuentra entre los siguientes 256 posibles códigos o hacer uso de un generador de números pseudoaleatorios tanto en receptor como transmisor. Este tipo de medida de seguridad es usada habitualmente en vehículos, alarmas y puertas automáticas.

Uno de las implementaciones más complejas es la llamada challenge-response, donde nuestra llave o *key fob*, en el caso de un vehículo, tiene capacidades tanto de emisión como de recepción y envía un mensaje al vehículo, siguiendo el mismo ejemplo, el cual genera un *challenge* o problema el cual es devuelto a la llave. Esta generará una respuesta (*response*) única a ese problema y la transmitirá al vehículo de nuevo. Si la llave no está asignada al vehículo en cuestión, la respuesta no se corresponderá con la esperada y no generará ninguna respuesta por parte de este último.

2.3.2. Zigbee

Zigbee es una tecnología de transmisión de datos por radiofrecuencia que usa las bandas de 868Mhz en el territorio europeo y 915Mhz en América, adicionalmente usa la banda 2.4Ghz de forma global.

Cabe destacar que Zigbee tiene dos vertientes diferenciadas Zigbee 3.0 que usa únicamente la banda 2.4Ghz y Zigbee PRO la cuál es usada en dispositivos de bajo consumo y sí que puede usar las otras dos bandas adicionalmente a la usada por Zigbee 3.0.

Entre las características destacables se encuentra su escalabilidad, la seguridad que ofrece a través de diferentes sistemas de cifrado, como AES-128. Además ofrece la posibilidad de la interconexión a modo de malla entre los diferentes dispositivos.

2.3.3. SigFox

Es otro de los sistemas que están implementándose actualmente en el terreno industrial. Consiste en la interconexión de los diferentes nodos SigFox para crear una red en forma de malla.

Esta tecnología permite la transmisión bidireccional de mensajes, pero tiene como restricción el envío de únicamente 140 mensajes de 12 bytes por jornada. Las frecuencias usadas son 868Mhz para Europa y 915Mhz en América moduladas en DBPSK o GFSK, con un ancho de banda de 100Hz, es decir, UNB (*Ultra Narrow Band*). Su distancia de transmisión efectiva puede variar entre 3 y 50Km, dependiendo de obstáculos y ruido electromagnético.

En el momento del envío de un mensaje, se envía una trama de datos la cual es replicada en tres frecuencias distintas de forma alterna, es decir, el envío no se realiza de forma simultánea por tres frecuencias. Sino que se realiza por una y se salta a la siguiente. Adicionalmente este mensaje se envía más de una vez para asegurar que ha sido recibido. Dado que usa un ancho de banda de únicamente 100Hz y el salto de frecuencias que realiza, se hace complicado usar técnicas de *jamming* con esta tecnología.

El uso de esta tecnología está especialmente indicado para IoT *Internet of Things*, aunque por el momento no está implantado en dispositivos móviles, solo en nodos de interconexión. Para un funcionamiento correcto la densidad de la red tiene que ser muy alta, por lo que su uso está especialmente indicado para el envío de ráfagas de mensajes de forma puntual.

Debido a que es una tecnología propietaria no se disponen de demasiados datos acerca del funcionamiento interno.

2.3.4. LoRa

Tecnología diseñada para la creación de redes de comunicación de bajo consumo o LPWAN (*Low Power Wide Area Network*).

Se divide en dos partes. LoraWAN, que define el protocolo de comunicación y la arquitectura para la red. Y la capa física LoRa, la cual establece el enlace para las comunicaciones de largo alcance. Dado que la parte relacionada con las comunicaciones por radiofrecuencia se engloban en LoRaWAN, esta será la parte a analizar.

La distribución de frecuencias varía según el país. Así en Europa se usan las frecuencias comprendidas entre los 867 y los 869Mhz, mientras que en Norte América estas van desde los 902 a los 928Mhz. Del mismo modo especificaciones como la cantidad de canales, el ancho de banda o la potencia de transmisión difieren entre países.

En el caso de Europa se dispone de 10 canales, con una potencia de emisión y recepción restringida a +14dBm. Ocho de estos canales tienen una transmisión que varía entre los 250bps y los 5.5kbps. En los otros dos esta velocidad difiere, siendo en ambos casos más alta, en uno de ellos de 11kbps y 50kbps con modulación FSK en el otro.

La modulación usada por LoRaWAN es *Chirp Spread Spectrum* (Chirp SS) o frecuencia modulada pulsada de espectro ancho. Consiste en la variación de la frecuencia de forma similar a FSK. De forma adicional se envía un pulso que recorre un rango de frecuencias. Una de las ventajas de esto es que dificulta usar técnicas de *jamming* en las comunicaciones.

Es un sistema ideal para la monitorización y accionamiento de actuadores, dado que la tecnología está diseñada en 3 grupos los cuales tienen diversas características en relación al consumo de energía.

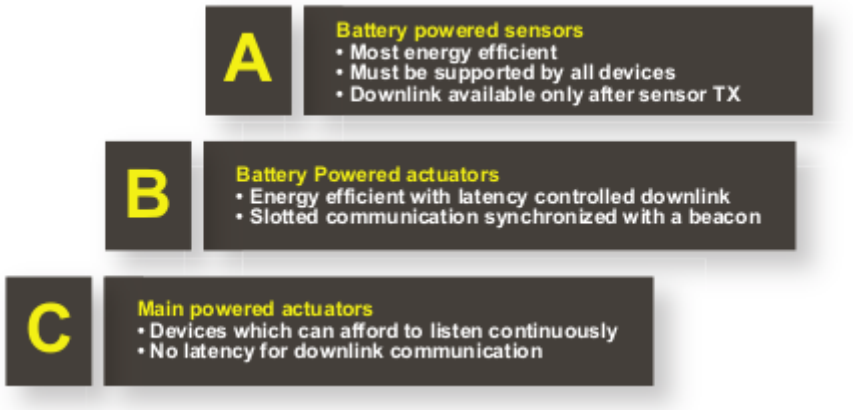

Figura 2.12: Uso de las clases de los dispositivos LoRa

En el caso del tipo A, prima la eficiencia energética. Es usada para sensorización alimentada a través de baterías. La restricción fundamental, que permite este bajo consumo, es que el enlace de descarga de datos hacia el sensor está disponible únicamente tras la transmisión por parte del sensor. El tipo B es usado en actuadores alimentados mediante baterías. El último tipo, el C, está especialmente diseñados para dispositivos actuadores que tienen una alimentación constante y se encuentran constantemente a la escucha de órdenes.

2.3.5. POCSAG

Este protocolo ha sido habitualmente usado por los "buscas", comúnmente llamados *beepers* o *pagers* en los países de habla inglesa, para el envío de mensajes, o pages, en una sola dirección. Esto quiere decir que desde el propio dispositivo receptor no se puede responder al mensaje en cuestión.

Las velocidades de transmisión de datos son 512, 1200 y 2400bps. Siendo la primera la que ofrece un alcance mayor, mientras las otras dos permiten más mensajes por segundo.

Las pages son transmitidas en grupos con un preámbulo al inicio de la estructura. Este hace que los dispositivos se pongan a la escucha para recibir el mensaje.

La base es una modulación FSK, aunque se puede modular de diferentes formas, trabajando en un régimen de frecuencias que está entre los 430Mhz y los 910Mhz, aunque estas pueden variar de forma significativa encontrándose emisiones en los 140Mhz y otras frecuencias.

Actualmente este protocolo sigue en uso debido al bajo coste de su implementación y puede verse a menudo en negocios relacionados con la hostelería, como pudieran ser restaurantes y hoteles, donde son usados a modo de avisador por los clientes o camareros. Así mismo es usado también por servicios médicos, en los que se envían los mensajes a la unidad móvil.

2.3.6. Project 25

También conocido como P25 o APCO-25 es un conjunto de estándares de radio digital. El uso principal de estos estándares está extendido por Norte América y Canadá. Tiene un uso similar a Tetra en Europa. Al igual que este es un sistema de radio troncalizada.

Opera de forma similar a la radio FM analógica, de hecho, permite operar en el modo analógico convencional, haciendo compatible la comunicación con dispositivos que operen en ese modo.

Cuando opera en modo digital la onda portadora usa cuatro frecuencias, lo que representa cuatro combinaciones de dos bits. Dado que el despliegue de P25 se realiza por fases, es necesario diferenciar que tecnologías son relativas a que fase.

Actualmente en la fase 1 se usa la modulaciín C4FM (*Continuous 4 Level Frequency Modulation*), similar a QPSK, donde los símbolos están desplazados 45 grados en la constelación y la amplitud de la portadora es constante. En esta fase los canales tienen un ancho de banda de 12,5Khz.

En lo que la fase 2 supone, los canales tienen un ancho de banda de 6.25Khz. Lo que permite cuatro conversaciones en el ancho de banda que utilizaría habitualmente un sistema analógico (25Khz). La modulación en esta fase es CQPSK, la cual se encarga de forma simultánea de modular la amplitud de la onda portadora y la fase. De forma adicional, en esta segunda fase las necesidades del bitrate se han visto reducidas gracias al uso del códec de voz AMBE+2.

Las frecuencias en las que se pueden encontrar las diferentes troncales pertenecen tanto a VHF como UHF y son las siguientes:

- 132 – 174Mhz
- 380 – 512Mhz
- 764 – 870Mhz

En lo que a la seguridad respecta P25, permite el uso de DES y AES como algoritmos de cifrado de extremo a extremo. De forma adicional se establece una especificación adicional para actualizar las claves de cifrado a través de la red de radio (OTAR, *Over The Air Rekeying*).

2.3.7. TETRA

También conocida como Radio Terrestre Troncalizada (*Terrestrial Trunked Radio*) o Radio Trans-Europea Troncalizada (*Trans-Euopean Trunked Radio*). Al contrario que Project 25 su uso está extendido por Europa. En el caso de España es usado por las fuerzas de seguridad del estado. Al igual que la fase 2 de P25 usa TDMA con cuatro canales por señal portadora espaciados, estas señales están espaciadas cada 25Khz.

Permite la emisión punto a punto o multipunto (*Point-to-Point* y *Broadcast*). Al contrario que su homólogo americano, no se puede realizar comunicación analógica, única-

mente se contempla el uso de la señal digital.

Las frecuencias sobre las que funciona TETRA son UHF, en España suele usarse entre los 380 y 460 Mhz, pero dependiendo del país se puede encontrar ubicado entre los 380 y los 470Mhz o los 806 y los 870Mhz.

La modulación usada por TETRA es 4QPSK. Permitiendo establecer cifrado AES y DES de extremo a extremo en sus comunicaciones.

2.3.8. D-STAR

Digital Smart Technologies for Amateur Radio (D-STAR) se trata de un protocolo de transmisión digital abierto. Las radios D-STAR pueden usarse tanto punto a punto como radio y repetidor, es decir, los usuarios pueden comunicarse entre ellos sin necesidad de hacer uso de un repetidor.

Existen dos modos de D-STAR, *Digital Voice* (DV) y *Digital Data* (DD). En el caso de DV, se utiliza 144 y 440MHz para la voz digitalizada (3600 bps) y para los datos digitales (1200 bps). Para la codificación, y posterior decodificación, del audio se hace uso del códec conocido como AMBER (*Advanced Multi-Band Excitation*). Este *codec* es la única parte propietaria del protocolo D-STAR.

En el caso de Digital Data, solo se hace uso de la banda de frecuencias ubicada en los 1.2GHz. Permitiendo transferencias de datos a 128kbps. En el caso de conexiones de baja velocidad es necesaria la conexión de la radio a través de una interfaz de puerto de serie o USB 1.0. Si, por el contrario, se quiere hacer uso de la conexión de alta velocidad, la conexión a la radio con el ordenador se realizará con un cable Ethernet convencional.

En ambos modos la modulación empleada será GMSK y hace uso de FDMA. Con un ancho de banda de 6,25khz por canal.

En caso de que la estación repetidora disponga de una conexión a internet, se podrá realizar un acceso a la red global a través de la conexión de radio. Esto permite, por ejemplo, el uso de mensajería instantánea a través de las interfaces de radio.

2.3.9. DMR

Digital Mobile Radio es un estándar de comunicaciones de radio publicado por la *European Telecommunications Standard Institute* (ETSI). Al contrario de D-STAR hace uso de TDMA en vez de FDMA y dispone de un ancho de banda de 12,5Khz (el doble que la primera). El rango de frecuencias del que puede hacer uso este estándar abarca desde los 30Mhz hasta el Ghz.

A causa del uso de TDMA es posible realizar dos conversaciones de forma simultánea haciendo uso de un único repetidor. En adición a esto, al ser totalmente digital y gracias a la optimización de los codecs de voz usados, la claridad de las transmisiones es mucho mayor que en sistemas analógicos.

En adición a todo esto, es posible el envío de mensajes de texto, similares a los conocidos SMS, entre los dispositivos.

En lo que respecta al acceso a internet desde los transmisores, si existe una unidad repetidora que tenga acceso a la red global, es posible realizar transmisiones a través de protocolos de red con todo el mundo.

2.3.10. GSM

GSM, por sus siglas en inglés de *Global System of Mobile Communications*, es un estándar europeo para redes de telefonía móvil con soporte para voz y datos.

La red GSM está constituida por diferentes células o estaciones base (*Base Stations* o *Base Transceiver Station*) que disponen del enlace por radio a los dispositivos móviles. Estas a su vez se enlazan con un conmutador que proporciona el acceso con la red de telefonía cableada.

Actualmente en España se hace uso de la red GSM 900, la cual opera en la frecuencia indicada por su propio nombre. Pero existen diferentes bandas en torno al globo que hacen uso de la red GSM, desde los 850Mhz hasta los 1900Mhz.

A causa de su extensa implantación, el uso del estándar es muy común, pudiéndose encontrar comunicaciones no solo de teléfonos móviles, sino de incluso de módems industriales que aprovechan la cobertura nacional existente para realizar enlaces de datos.

2.4 Vulnerabilidades genéricas

El inconveniente principal de muchas de las tecnologías que hacen uso de las radiofrecuencias es su antigüedad y estancamiento, considerándose muchas de ellas seguras por estas mismas razones. Pero más allá de lo que pudiera parecer seguro en un principio es necesario tener en cuenta que algunas de ellas tienen más de 10 años y lo que en esa época se consideraba impensable de alcanzar hoy en día lo consideramos como algo normal.

2.4.1. Interferencias

El inconveniente general del uso de sistemas de comunicación por radio son los fallos producidos por interferencias. Estas pueden ser producidas por sistemas eléctricos causados por una instalación eléctrica que no ha sido correctamente instalada o incluso por sistemas de iluminación que hacen uso de transformadores eléctricos y/o inversores de corriente (usados en tubos de fluorescentes, por ejemplo).

En lo que a la parte intencional de la generación de interferencias se refiere, podemos definir a estos dispositivos como inhibidores de frecuencia. Realmente no inhiben una frecuencia, puesto que esta no desaparece del espectro por razones obvias, sino que emiten interferencias, "ruido" en la mayor parte de los casos, sobre una banda de frecuencias en concreto. Esta emisión genera una saturación de la frecuencia haciendo impracticable la escucha, en el caso de audio o la recepción de los mensajes en caso de datos (denega-

ción de servicio).

El uso de un inhibidor o *jammer* no está únicamente relevado a su uso contra walkie-talkies, telemandos o telefonía móvil, dado que dependen de la frecuencia para la cual ha sido diseñada se puede usar en todo el espectro que abarque el dispositivo.

Actualmente el uso de esta clase de dispositivos se considera ilegal en España, permitiéndose su uso a las Fuerzas y Cuerpos de Seguridad y Administraciones Públicas autorizadas, el uso de dispositivos de esta clase debe ser autorizado expresamente por la Secretaría de Estado de Telecomunicaciones.

2.4.2. Errores de configuración

Muchos de las tecnologías nombradas previamente proporcionan algún tipo de cifrado para securizar la transmisión y evitar que, pese a que se pueda interferir, se obtengan datos que puedan ser provechosos de alguna forma para un posible atacante.

Por poner algunos ejemplos, tecnologías como TETRA o Zigbee proporcionan la posibilidad de cifrar sus comunicaciones, pese a esto no es algo que se suela hacer, ya sea por desconocimiento de que ofrecen esta característica o porque, como en el caso de algunos dispositivos dotados de Zigbee, el fabricante considera que los datos a transmitir carecen de la condición para aplicar este extra se seguridad.

2.4.3. Fallo en el protocolo

Del mismo modo que hay sistemas WiFi que son vulnerables a algunos ataques a causa de su protocolo, encontramos que hay otras tecnologías de radio que también lo son. Un claro ejemplo de esto es, en tecnologías explicadas anteriormente, los códigos estáticos en los telemandos.

CAPÍTULO 3
Procedimiento a seguir

A continuación se detallarán con el máximo detalle posible los procedimientos a seguir para poder realizar el análisis de las tecnologías nombradas anteriormente y comprobar si son realmente seguras en las aplicaciones que se están usando.

Previo a los diferentes pasos a seguir se realizará una breve explicación del material y requisitos necesarios para poder realizar estos.

3.1 Prerrequisitos y material necesario

3.1.1. Hardware

Las necesidades de hardware necesarias para identificar e interceptar transmisiones de radio varían en gran parte de la frecuencia y modulación objetivo. Así en algunos casos con un escáner, como el nombrado anteriormente3, será suficiente para captar el audio, pero insuficiente para otros tipos de modulaciones u otro rango de frecuencias.

Los elementos básicos de los que se debe disponer son:

- Antena/s. Deben corresponderse con la frecuencia que se quiere analizar.

Figura 3.1: Antenas de diferentes frecuencias

- Software Defined Radio (SDR). Permite modificar la frecuencia a sintonizar en un amplio rango, habitualmente este va desde los 30Mhz a los 1.2Ghz en los equipos más sencillos.

Figura 3.2: SDR usado durante el proyecto

- Escáner. Al hacer uso de este tipo de dispositivos se obtiene la ventaja de recibir muchas frecuencias en un corto periodo de tiempo, en algunos casos de hasta 300 frecuencias por segundo con una diferencia de 5Khz entre ellas.

Figura 3.3: Escáner ICOM R-6

Figura 3.4: Radio DMR Retevis con *firmware* modificado para escanear DMR

- Ordenador. Al hacer uso de un SDR es necesario disponer de un quipo con unas características mínimas, procesador con dos núcleos y al menos dos gigabytes de memoria RAM. El uso que se le dará a este es el de procesar los datos recibidos a través del SDR en cuestión.

Como se ha indicado previamente, en lo que se refiere a las antenas a usar, es necesario tener en cuenta que frecuencia es la que se quiere analizar. Así pues para una antena omnidireccional diseñada para una frecuencia de 433Mhz la longitud diferirá de una que sea usada para 1.2Ghz. La relación de longitud-frecuencia para las antenas es la siguiente, donde indica la longitud de onda, la frecuencia requerida en Mhz y es la longitud de la antena en metros:

$$Long = \lambda/4 = (\frac{300}{freq})/4$$

Existe casos en los cuales la longitud de la antena, debido a su diseño, puede ser modificada, son las conocidas como antenas extensibles. Estas tienen un rango de acción diverso, pero siempre tienen unos límites máximos y mínimos los cuales se restringirán a la misma relación frecuencia-longitud

En el caso de hacer uso de antenas direccionales, su construcción también varía dependiendo de la frecuencia. Dependiendo del diseño escogido las relaciones difieren unas de otras.

Como se ha indicado anteriormente, el uso de un escáner tiene la ventaja que se puede registrar un rango concreto de forma automática. Estos rangos pueden ser programados en el dispositivo, así como la diferencia o *steps* entre las frecuencias. Como contraparte la mayoría de equipos de estas características están diseñados para demodular FM, por lo que todo lo que no corresponda a esta modulación no será identificable fácilmente. Aun así es posible identificar si se está realizando algún tipo de transmisión e inferir, teniendo en cuenta el contexto, de que tecnología se trata.

Figura 3.5: Antena extensible usada durante el proyecto

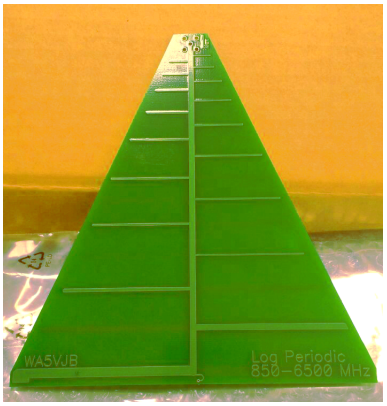

Figura 3.6: Antena logoperiódica

En algunos dispositivos de escaneo, se ofrece por parte del fabricante una interfaz de conexión a un ordenador para programar el dispositivo e incluso para obtener datos en tiempo real de las frecuencias y/o realizar grabaciones de lo sintonizado.

3.1.2. Software

En lo que a software se refiere es necesario disponer de un sistema operativo basado en Linux, las pruebas se han realizado con Ubuntu 14.04 y 16.04.

Para el análisis e identificación de las diferentes frecuencias y tecnologías el uso de herramientas como GQRX (en sistemas Linux) y SDR Sharp (para equipos con sistema Windows). En estos programas se puede hacer una búsqueda de la frecuencia concreta para localizar su centro, así mismo se muestra un waterfall la cual facilita la interpretación. Adicionalmente estos dos programas disponen de plugins de terceros que añaden funcionalidades adicionales.

Para realizar la demodulación e interceptación es necesario el uso de la aplicación GNURadio. Esta usa la programación por bloques, mediante la que se pueden desarrollar programas de una forma rápida. Adicionalmente existe una comunidad de desarrolladores tras GNURadio la cual ha creado sus propios bloques de programación para añadir más funcionalidades.

De manera paralela a la aplicación mencionada anteriormente existe una similar, LuaRadio. Ofrece características similares a GNURadio, con la ventaja que requiere menos capacidad de computo pero como desventaja no hay una comunidad desarrollo tan amplia.

Adicionalmente es necesario hacer uso en Linux de las librerías específicas para RTL-SDR, como libsdr o gr-osmosdr. Así como librerías para poder mostrar el espectro de las frecuencias como fftw o VOLKS.

Para la interceptación se requieren de diferentes herramientas software que serán indicadas en cada uno de los correspondientes apartados a cada tecnología.

3.1.3. Marco legal

Dado que se hace uso de diferentes frecuencias es necesario tener un conocimiento previo de las leyes que aplican a cada país en este campo. En el caso de este proyecto la se tendrá en cuenta únicamente la normativa vigente en el territorio español, siendo esta la publicada en el Boletín Oficial del Estado (BOE) número 114, con fecha 10 de mayo de 2014.

Ha considerar tienen los artículos en los cuales se definen las infracciones y su categorización. Estos van desde el art.76, que se corresponde con las infracciones muy graves hasta el 78, donde se indican las leves. En los posteriores artículos se explica e indica en qué consisten las sanciones y el método sancionador.

A destacar entre las diferentes sanciones dentro de las identificadas dentro de la categoría de graves la que se corresponde al punto 4 del artículo 77.

> "4. La mera producción, en España o en los países vecinos, de interferencias definidas como perjudiciales en esta Ley que no se encuentren comprendidas en el artículo anterior."

En lo que refiere a las sanciones tipificadas como muy graves, se debe destacar sobre el marco general las siguientes, indicadas todas ellas en el artículo 76:

> "1. La realización de actividades sin disponer de la habilitación oportuna en las materias reguladas por esta Ley, cuando legalmente sea necesaria"
> "4. La utilización del dominio público radioeléctrico, frecuencias o canales radioeléctricos no adecuada al correspondiente plan de utilización del espectro radioeléctrico o al Cuadro Nacional de Atribución de Frecuencias"
> "10. La interceptación, sin autorización, de telecomunicaciones no destinadas al público en general, así como la divulgación del contenido"

En algunos de los puntos referentes a las infracciones se hace mención al Cuadro Nacional de Asignación de Frecuencias (CNAF). En este se indican las frecuencias y requerimientos para la utilización de estas. Así mismo, anexo al CNAF existen las Notas de utilización nacional (UN) en la que se indican variaciones y correcciones respecto de las tablas de atribución de frecuencias del CNAF.

3.2 Reconocimiento

A causa de la diversidad de tecnologías que hacen uso de las ondas de radio para la transmisión de datos se ha examinado el uso de las más comunes y extendidas, tanto en ambientes domésticos como empresariales.

3.2.1. Telemandos

Debido a que su uso está destinado a emisiones de corta distancia, como se ha explicado previamente, el rango de frecuencias que se usa es muy amplio. Siempre que pueda identificarse visualmente el telemando o al menos la marca de este nos será de gran ayuda.

Cabe recordar que dependiendo del continente las frecuencias de uso pueden variar, siendo las más comunes 315Mhz (EEUU y Asia), 433Mhz y 868Mhz (ambas para Europa). Pese a esto es posible encontrar que fabricantes asiáticos o americanos de automóviles mantengan esas frecuencias en Europa.

Si se dispone de una imagen del dispositivo físico es posible identificar que frecuencias usará a través de una búsqueda en internet. En caso de tener acceso físico al dispositivo se hace más sencillo ya que en muchos dispositivos se indica la frecuencia o la banda de trabajo asignada.

En caso de que no se disponga de ninguno de estos datos será necesario analizar estas frecuencias hasta dar con la frecuencia exacta que se está usando.

Un ejemplo es el que se observa en las figuras al final de la sección. Se puede ver claramente que la frecuencia, en este caso en la banda 433, no se ajusta exactamente a los 433Mhz.

El mayor inconveniente para realizar este tipo de identificación es que suele ser muy breve dado que suele ser usado en apertura de puertas a distancia de garajes y vehículos o alarmas de estos, con el añadido de que cada fabricante puede usar una señal de mayor o menor amplitud y/o una transmisión que puede variar en duración de unos a otros. Si se comparan ambas figuras, se ve claramente que las señales no se parecen ni en su amplitud, ni en su duración, ni en la frecuencia pese a estar en la misma banda. En el caso de la segunda figura la modulación es AM, mientras que en la primera es una variación de FSK, concretamente 2FSK.

Por tanto es necesario si se desconoce de qué dispositivo se trata intentar inferir el tipo de modulación que está empleando.

Al hablar previamente de los telemandos se ha explicado que existen diversas implementaciones y que estas aplican diferentes métodos de autenticación, es importante tener esto en cuenta. Puesto que, en ciertos casos, lo mostrado en el *waterfall* puede ser a causa de una comunicación bidireccional, como pudiera ser en el caso de la autenticación *challenge-response*.

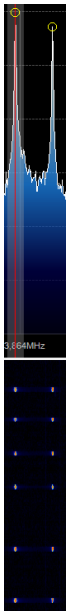

Figura 3.7: Emisión de telemando de Suzuki

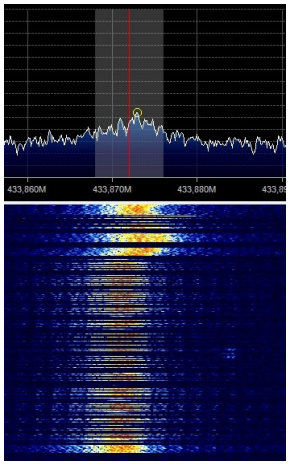

Figura 3.8: Emisión de telemando de BMW

3.2.2. ZigBee

Actualmente la identificación de sistemas ZigBee, pasa por hacer uso de un módulo, en su versión pro o en su versión 1, con la consecuente diferencia de frecuencias. Y analizar el funcionamiento que hacen cada uno, el mayor problema de esta tecnología es que la mayor parte del tiempo los módulos se encuentran en estado de hibernación. Por lo que haciendo uso de un SDR se hace virtualmente imposible captarlos.

Pese a esto, es posible, mediante la modificación de kits de desarrollo producidos por Texas Instruments, interceptar transmisiones que hagan uso de esta tecnología. Para lo cual la propia empresa proporciona las herramientas software necesarias.

Adicionalmente, existe un proyecto, de nombre KillBee, el cual hace hincapié en la seguridad de ZigBee. Y en el cual han desarrollado herramientas tanto hardware como software para esta tecnología.

Es necesario tener en cuenta que pese a las diferentes herramientas desarrolladas, ya sea por equipos de desarrolladores ajenos a los fabricantes de dispositivos o por estos mismos, debido al uso que se hace de ZigBee es necesario encontrarse muy próximo a la fuente de emisión, por tanto es necesario tener el conocimiento de donde se encuentra esta.

3.2.3. Sigfox

Usando las mismas bandas que LoRa, el problema de su identificación radica precisamente en una de sus bases, solo se pueden enviar como máximo 144 mensajes de 12 bytes lo cual hace que captar su emisión sea mucho más complicado.

En lo que a la identificación visual respecta, el *waterfall* resultante de captar su transmisión es el mostrado en la siguiente ilustración.

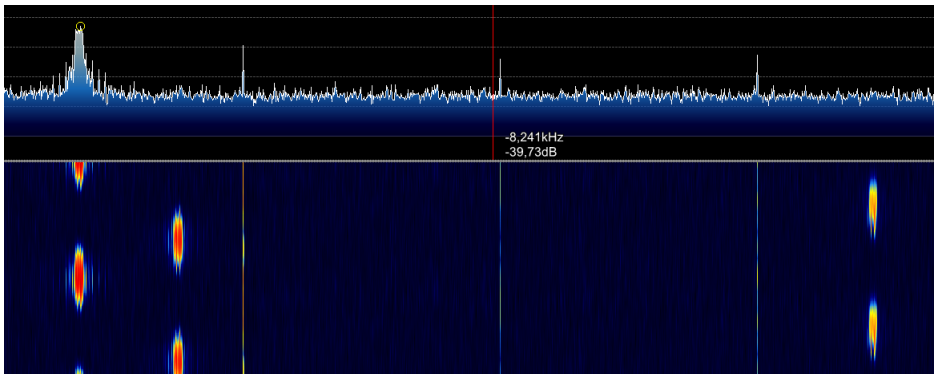

Figura 3.9: Sigfox waterfall

En la imagen previa se observa que tras la finalización de una ráfaga se realiza una segunda con su frecuencia desplazada.
Una de las ventajas de intentar identificar SigFox es que dispone de un mapa de la cobertura actual del protocolo.

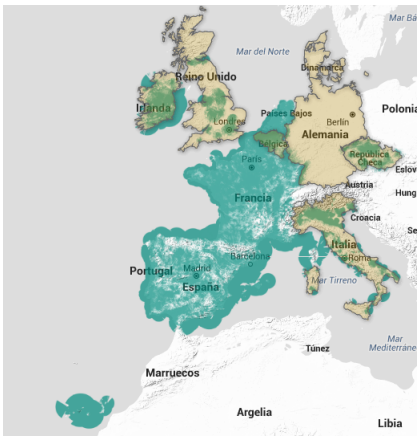

Figura 3.10: Mapa de cobertura Sigfox

3.2.4. LoRa

La identificación de LoRa, una vez localizada su frecuencia resulta relativamente sencilla a causa del peculiar preámbulo usado por el protocolo fácilmente identificable en el waterfall de la aplicación, tal y como se puede observar en la siguiente ilustración.

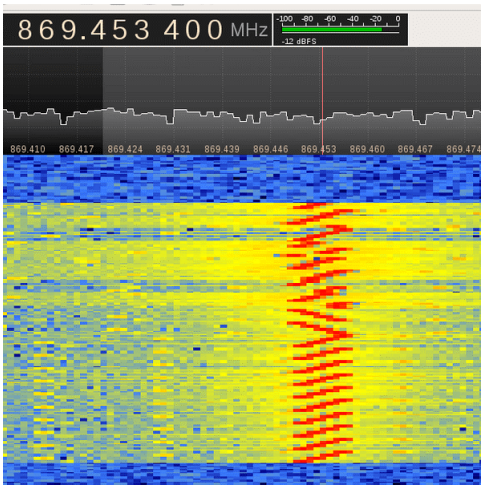

Figura 3.11: Preámbulo de LoRa

La complejidad pues de este protocolo radica en identificar la frecuencia exacta, pero recordemos que la regulación de LoRa implica que se usa la banda 868, con lo que la identificación, en caso de captar la señal, es reconocible de forma visual con una relativa facilidad.

3.2.5. POCSAG

Tal como ocurre con las señales de LoRa o Sigfox, este tipo de transmisiones suele ser intermitente y únicamente se realiza cuando es necesario comunicarse con uno o varios dispositivos (*pagers*). Pero al contrario que las dos indicadas, suele ser más común su uso y es común que se envíen repetidas veces en bucle los mensajes por un periodo determinado de tiempo, para así poder asegurar que el receptor lo recibe.

Al contrario que TETRA o P25 en estas transmisiones no se envía ningún tipo de mensaje de audio. Únicamente es posible el envío de mensajes alfanuméricos o numéricos En los casos en los que el dispositivo receptor dispone de pantalla estos mensajes serán mostrados. En caso contrario siempre y cuando se haya indicado, en los bits dedicados para ello en la trama, se emitirá un pitido, vibración o zumbido.

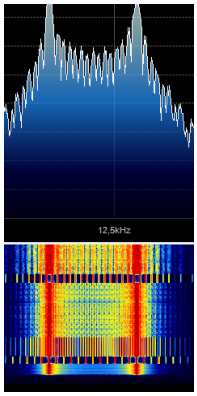

Figura 3.12: Ejemplo de señal POCSAG

El waterfall generado es bastante identificable. Hay que tener en cuenta que este se emite durante un breve periodo de tiempo y será anómalo si no existe ningún tipo de transmisión en la banda de frecuencia que se está analizando. En la imagen previa se puede comprobar que la modulación usada es FSK.

3.2.6. P25, D-STAR y DMR

Debido a que P25, D-STAR y DMR son sistemas digitales, el reconocimiento de todos ellos es similar pese a hacer uso de diferentes tecnologías para la asignación de los canales o diferentes anchos de banda.

En todos los casos el audio que se capta, sin hacer uso de un *vocoder* y el *waterfall* que se observa en el momento de captar una de estas tecnologías, es muy similar por lo que es necesario hacer uso de herramientas adicionales y tener en cuenta donde son comunes sus usos, es decir, el contexto de la emisión.

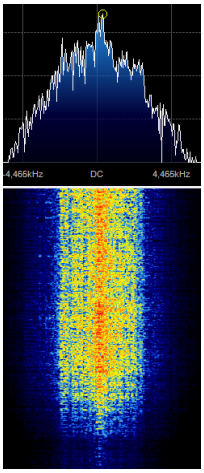

Figura 3.13: Ejemplo de señal P25

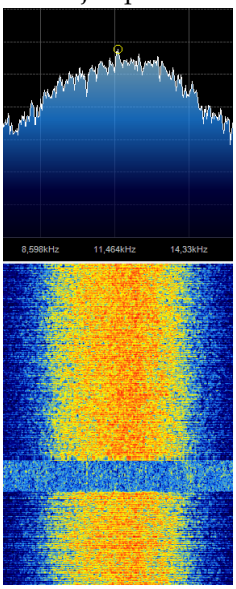

Figura 3.14: Ejemplo de señal DMR

A causa de que no es un estándar en Europa, es difícil encontrar este tipo de transmisiones en nuestro país. Actualmente la mayor cantidad de equipos y redes que pueden interactuar con P25 se encuentran distribuidas por Norte América, América Latina, el territorio soviético, Asia y la mayor parte de Oceanía.

Pese a esto, no es imposible captar emisiones debido a la importación desde EEUU y los países asiáticos.

DMR está extendido por todo el territorio europeo y EE.UU. Los repetidores de las tres redes que hacen uso de DMR (DMR-Marc, DMR+ y BrandMeister) se encuentra mapeada a nivel mundial.

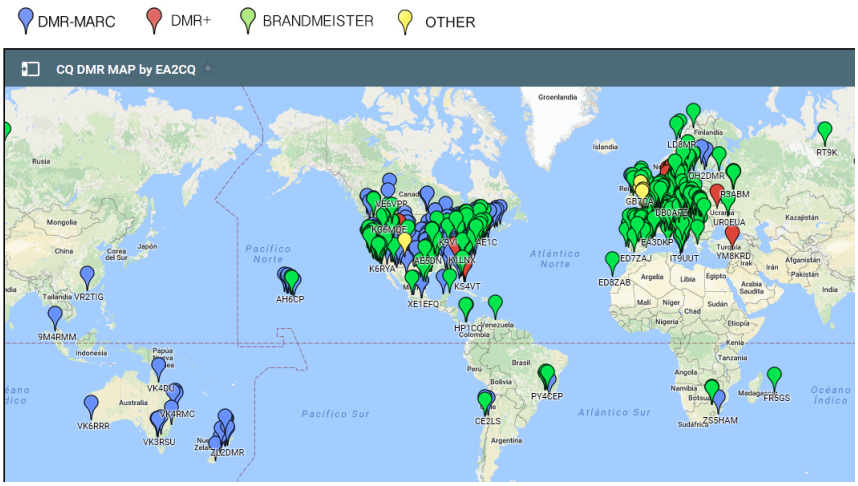

Figura 3.15: Mapa de repetidores de DMR

En el caso de D-STAR el uso que se hace es entorno a todo el globo, por lo que no debería descartarse en ningún momento que la señal identificada fuese esta tecnología.

En lo que a la identificación se refiere el reconocimiento del audio es muy poco característico. Unido a que puede realizar emisiones tanto analógicas como digitales hace aún más compleja su identificación. Siendo la forma más sencilla la utilización de un *vocoder* o en caso de que se use en modo analógico, simplemente analizando la señal como si se tratase de una emisión FM convencional.

3.2.7. TETRA

En España las frecuencias usadas por TETRA empiezan en la banda 390 hasta la 460 aproximadamente. Dado que es radio "troncalizada" a pesar de que se realice una transmisión de audio no podrá percibirse nada relevante únicamente demodulando la frecuencia, será necesario el uso de software adicional, un *vocoder (voice coder)*, para decodificar el audio y obtener una salida interpretable de la emisión.

Pese a las ventajas que ofrece esta tecnología respecto de las otras nombradas, uno de los grandes inconvenientes, por así decirlo, se debe a que el usuario no hace uso de todas las características que posibles. Una de las más importante es la que posibilidad de cifrar las comunicaciones.

Pese a que en la legislación española referente a telecomunicaciones se indica explícitamente que todas las comunicaciones han de ser realizadas sin cifrar, es posible realizar un cifrado de estas siempre que las claves de cifrado se hagan públicas.

Así mismo, hay que tener en cuenta que ciertas comunicaciones se sobreentiende que pueden ser cifradas sin necesidad de hacer públicas los sistemas usados para su securización dado el ámbito de uso. Un claro ejemplo de estas comunicaciones son las realizadas por los cuerpos y fuerzas del estado.

Durante las pruebas realizadas se han identificado transmisiones las cuales se han interpretado como pertenecientes a las FFCC del estado. A causa de que las frecuencias usadas no son públicas no es posible afirmar el origen. En la mayor parte de estas comunicaciones no se han usado las características de cifrado para aumentar la seguridad.

Hay que recordar que en el caso de las comunicaciones de las FFCC del estado, la divulgación de estas es completamente ilegal según la legislación vigente.

De estas transmisiones se extrae que, más allá de las comunicaciones de voz, es posible obtener información de los mensajes enviados. Entre estos datos se incluyen la posición, en tiempo real, de los activos involucrados en el intercambio de información.

Más allá de lo que a legislación se refiere, la identificación de las señales de TETRA es un tanto compleja. En caso de que se esté usando un programa similar a GQRX o SDRSharp, donde se busca un patrón distintivo en el waterfall, la dificultad radica en que en la banda de los 400Mhz se encuentran muchas emisiones que pueden ser fácilmente malinterpretadas como TETRA, por tanto la manera correcta de identificar este tipo de emisiones es a través del reconocimiento del patrón de la señal.

El patrón de la señal en el waterfall es similar a la mostrada en tecnologías como P25 o DMR, pese a que se trata de tecnologías que difieren entre ellas. La forma de la señal en el waterfall de GQRX es como el indicado en la siguiente imagen.

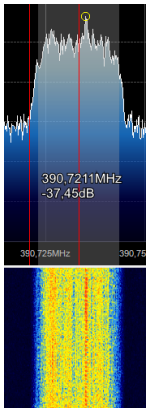

Figura 3.16: Ejemplo de waterfall de TETRA

La señal es relativamente simétrica y cuadrada, con un ancho de banda considerable. Pese a que se localice, hasta que no se intercepte, haciendo uso del correspondiente *vocoder*, no se puede asegurar que sea este protocolo.

3.2.8. GSM

Debido a que la emisión en de tráfico GSM está restringida por el Ministerio de Energía Industria y Turismo, es posible referirse a los documentos emitidos por ellos para

conocer las frecuencias en las que se puede realizar la emisión y por tanto acotar a estas frecuencias la búsqueda. Adicionalmente existen publicaciones actualizadas que recogen las bandas de frecuencias en las que emiten cada una de las compañías autorizadas en diferentes países.

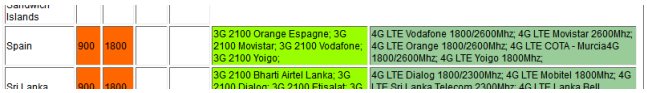

Figura 3.17: Frecuencias usadas en comunicaciones móviles en España. En naranja las correspondientes a GSM

Conociendo la banda de la cual se está haciendo uso es posible, mediante herramientas software como GQRX o SDR#, encontrar el centro de la frecuencia de esa emisión.

Estas bandas de frecuencias se dividen en canales, de forma similar a los puntos de acceso wifi, correspondiendo cada uno de estos canales a una estación base o BTS (*Base Transceiver Station*). Estando estas últimas en canales distintos a las estaciones vecinas que se encuentran dentro de su rango de alcance para evitar un solapamiento de las frecuencias.

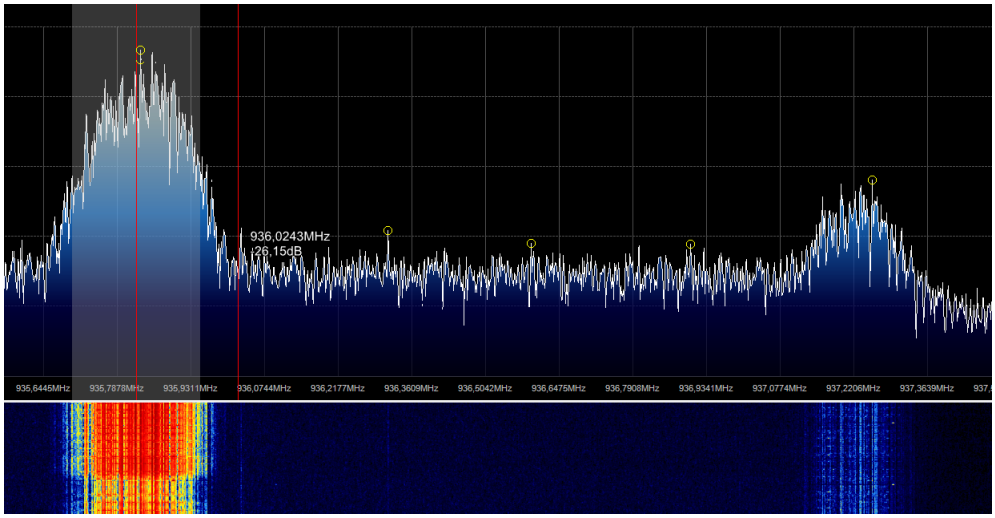

Figura 3.18: Señales GSM localizadas con SDR#

Del mismo modo que existen herramientas visuales que necesitan de la búsqueda manual de los canales, existen programas que, pese a no ser la búsqueda de canales GSM su función, permiten automatizar el proceso de obtención de estos haciendo más sencilla la identificación.

Uno de estos programas es Kalibre-RTL, de Joshua Lackey y Steve Markgraf. La función de esta herramienta es calibrar el SDR obteniendo con exactitud la variación respecto la frecuencia real que usa el BTS, permitiendo así compensar el error que tienen este tipo de dispositivos.

```
Found 1 device(s):
  0:  Generic RTL2832U OEM

Using device 0: Generic RTL2832U OEM
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
Setting gain: 42.0 dB
kal: Scanning for GSM-900 base stations.
channel detect threshold: 312357.587344
GSM-900:
        chan: 9 (936.8MHz + 313Hz)      power: 2886529.58
        chan: 20 (939.0MHz + 427Hz)     power: 2749105.44
        chan: 100 (955.0MHz + 837Hz)    power: 3097730.15
        chan: 120 (959.0MHz +  38Hz)    power: 707295.20
```

Figura 3.19: Herramienta Kalibre-RTL en funcionamiento

3.3 Interceptación

En términos generales, a causa de que el medio de transmisión de los mensajes es el aire, es posible interceptar todas las señales de cualquier tecnología de radio para su posterior análisis. Se puede considerar a grandes rasgos como interceptar señales de redes WiFi.

A continuación se exponen algunas de las tecnologías indicadas previamente y los métodos de análisis de estas.

3.3.1. Telemandos

A causa del amplio abanico de modulaciones y elementos de seguridad existentes aplicados por cada uno de los fabricantes de estos dispositivos, es muy complejo interceptar el contenido de las transmisiones.

Basándose en el método más simple, la modulación OOK, o lo que es lo mismo, la codificación ASK llevada al extremo. Se comprobará en el espectrograma de la señal capturada las frecuencias altas y bajas. Habitualmente las altas equivalen a un 1 digital, mientras que las bajas equivalen a un 0.

Dado que puede aparecer más de un valor igual consecutivo, es necesario conocer el sample rate para conocer la cantidad de valores iguales consecutivos que existen.

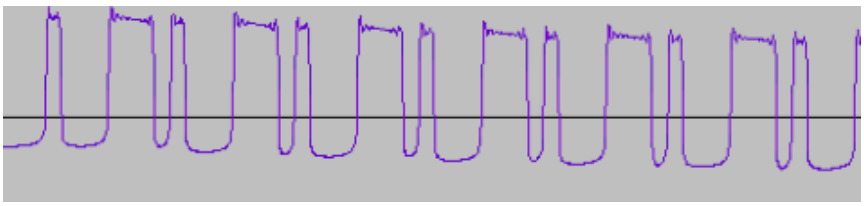

Figura 3.20: Contenido de una transmisión modulada en OOK

Para esta tarea existen herramientas automáticas como pueden ser rtl_433 o DecodeOOK. Pero dado que no existen estándares como tal para las aplicaciones que hacen uso de esta modulación, en la mayor parte de los casos será necesario obtener la emisión en binario para su posterior interpretación.

3.3.2. TETRA

Una vez haya sido presuntamente identificada la frecuencia correspondiente a la emisión TETRA, es necesario usar un vocoder para confirmar esta. Actualmente existen diversos paquetes de software, tanto comerciales como gratuitos, para decodificar los datos de la emisión.

En este caso para la interceptación se usará la herramienta telive, Tetra Live Monitor, desarrollada por Jacek Lipkowski. Este software permite mostrar la información de la señal, las comunicaciones y realizar escucha del audio.

Para realizar estas funciones se ayuda de GNURadio, haciendo uso de un conjunto de bloques concretos para la sintonización de la frecuencia exacta.

Para obtener los resultados deseados es necesario que la frecuencia sintonizada sea virtualmente simétrica. Esta señal se verá en la interfaz del programa en GNURadio de forma similar a la indicada en la siguiente imagen.

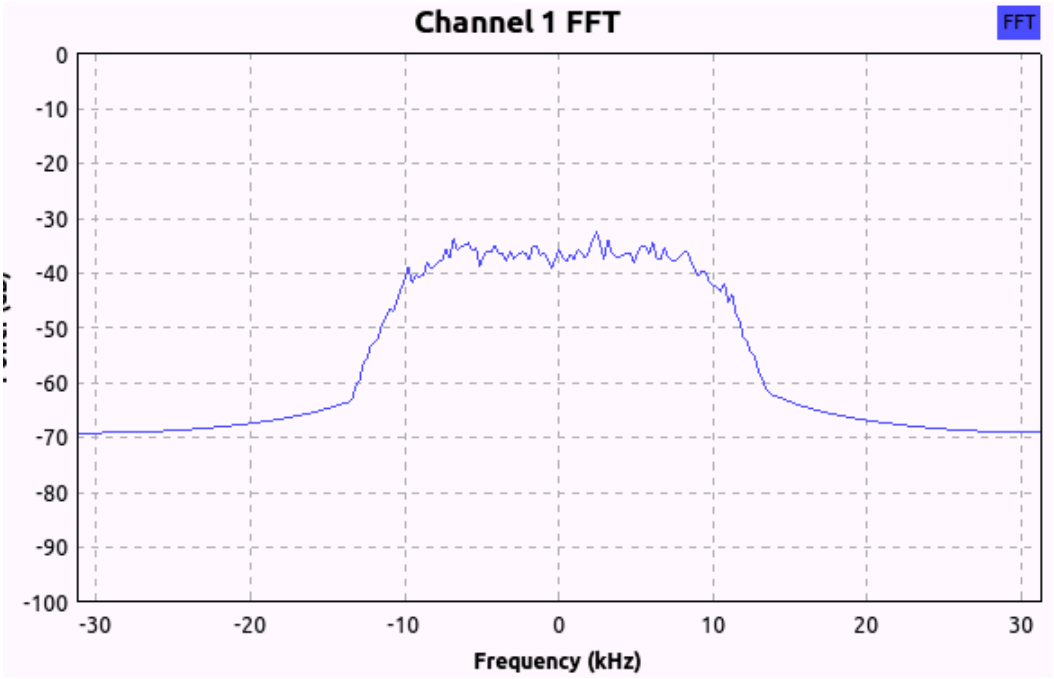

Figura 3.21: Frecuencia sintonizada correctamente en GNURadio

Adicionalmente a la simetría, es necesario que la señal alcance una potencia mínima. Según las experiencias, esta debe ser de al menos -40dB. En cuanto más potencia tenga la señal con menos interferencias se recibirá esta.

Habiendo localizado y configurado correctamente los valores ,la ventana de Xterm mostrará algo similar a la siguiente figura. Donde se muestra cada uno de los canales que está en transmitiendo en ese momento.

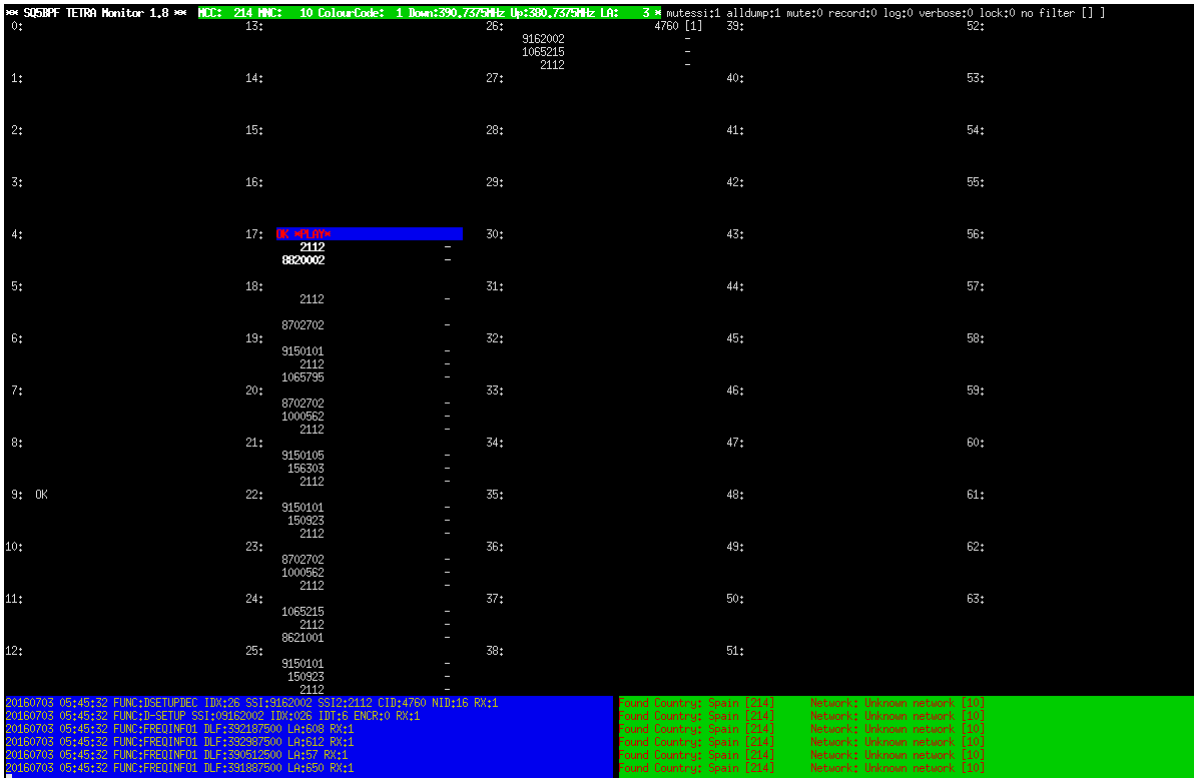

Figura 3.22: Canales en uso en Xterm

En la parte inerior se muestran datos de interés, como la posición de GPS de la transmisión y el SSI (*Short Subscriber Identity*) o identificador de quien inicia la transmisión, así como algunos adicionales (velocidad, cifrado…). De forma similar, en este mismo terminal, es posible acceder la información de cada uno de los canales, con las frecuencias exactas de cada uno de ellos, y la información sobre la recepción.

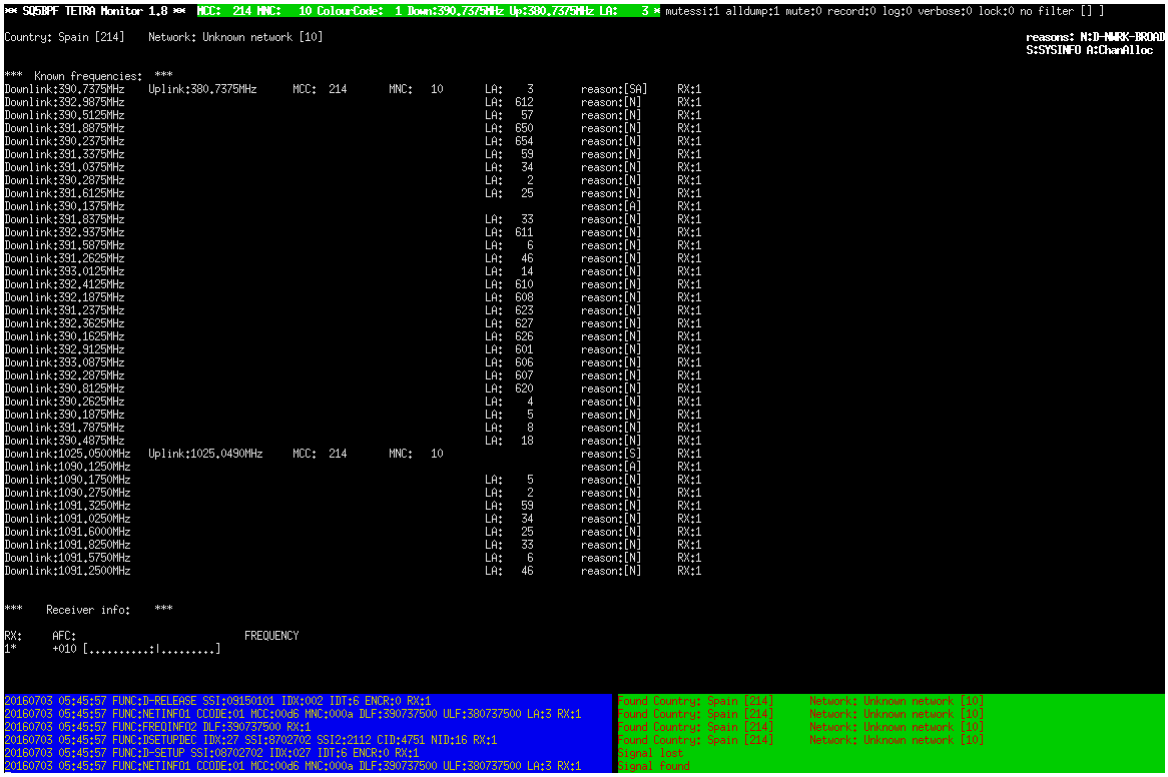

Figura 3.23: Información de los canales

En la imagen anterior se muestra cada uno de las frecuencias de los canales de los que se ha obtenido información. En el caso de que el canal esté en uso también se mostrará la frecuencia del *Uplink*.

Por supuesto, si no existe cifrado en el canal y se obtiene el audio este puede ser grabado para su posterior análisis, así como los *logs* de las transmisiones.

3.3.3. POCSAG

En el caso de POCSAG la modulación típica es FSK, donde la frecuencia más alta producida durante la modulación suele representar un 0 y la baja un 1 digital. Existen tres estándares, los cuales se diferencia entre ellos en la velocidad de transmisión. Estas son 512,1200 y 2400 bps. En el caso de hacer uso de 512 bps se obtiene un alcance mayor, mientras que con las dos restantes, 1200 y 2400, se pueden enviar más "páginas" por segundo.

La estructura de la transmisión se realiza en bloque. Donde existe un preámbulo de 576 bits, alternados entre 1 y 0 (e.g. 10101…). Se realiza de este modo para que los dispositivos ahorren energía. Normalmente se encuentran en standby y tienen periodos en los que están "despiertos". Durante estos periodos el dispositivo recibe la trama de bits alternos, la cual identifica la velocidad de transmisión y se sincroniza con esta.

Tras el preámbulo se envía (en la misma estructura) el *Frame Synchronization Code Structure* o FSC. Que está formado por 32 bits y tiene como función identificar el inicio de cada uno de los bloques, o *batch*, de la estructura de la transmisión.
En cada bloque existen dos tipos de palabras clave, la primera la dirección y el segundo

el mensaje. Ambos con una longitud de 32 bits de información.

La dirección es única de cada dispositivo y en caso de coincidir con la contenida en el mensaje enviado, este último alertará de que existe una transmisión dirigida hacia él por medio de un pitido, o a través de una pantalla en el caso de que se disponga de esta funcionalidad.

Si dispone de la funcionalidad para mostrar los mensajes este será el que se indica en el mensaje. Los mensajes pueden ser tanto alfanuméricos como únicamente numéricos. La codificación usada para cada uno de los caracteres es BCD con 4 bits.

Dada la gran cantidad de información que existe acerca de este protocolo hay multitud de programas los cuales identifican cada una de las tramas para que sean de fácil entendimiento.

En casos concretos como pudiera ser SDRangeLove (herramienta similar a GQRX o SDR#) incluso se ha integrado la decodificación de este tipo de transmisiones. En otras soluciones software, como LUARadio, ya existen bloques preprogamados que tienen dicha funcionalidad.

Por otro lado existe la posibilidad de hacer uso de multimon-ng el cual tiene funcionalidades adicionales y no requiere de GNURadio.

Por comodidad y debido a que este tipo de transmisiones son de carácter intermitente se recomienda realizar una captura en formato raw para posteriormente decodificarla con el software escogido.

```
POCSAG1200: Address: 1124565  Function: 3  Numeric: 140143 4[4
POCSAG1200: Address: 1124565  Function: 3  Alpha:   A Patient
POCSAG1200: Address: 1124565  Function: 3  Skyper:  @<US>O`shd
POCSAG1200: Address:      53  Function: 3  Alpha:   Unit: TAM2
Destination: 13:08<EOT><EOT>
```

Figura 3.24: Resultado obtenido con Multimon-NG

3.3.4. P25

Para la interceptación de P25, al igual que para TETRA, es necesario disponer de un *vocoder* para obtener el audio de la señal digital.

Una de las herramientas software más utilizada y mejor documentada hasta la fecha es *Digital Speech Decoder* (DSD). La cual entre otros protocolos permite decodificar las transmisiones de P25 fase 1 que no se encuentren cifradas.

Esta decodificación se puede realizar en tiempo real, redirigiendo por ejemplo la salida de audio de GQRX o SDRSharp hacia la instancia de DSD en ejecución.

Entre las diferentes opciones que tiene la herramienta se encuentran las que permiten mostrar el identificador del *talkgroup*. Una vez se está decodificando la emisión obtene-

mos datos de la modulación, si la transmisión es cifrada, el origen...

```
Sync:  +P25p1     o: 1408 mod: QPSK g: 25.000000 inlvl: 23% nac:  1F5 src:        0 tg:     0
Sync:  +P25p1     o:   24 mod: QPSK g: 25.000000 inlvl: 19% nac:  1F5 src:        0 tg:     0
Sync:  +P25p1     o:   24 mod: QPSK g: 25.000000 inlvl: 24% nac:  1F5 src:        0 tg:     0
Sync:  +P25p1     o:   24 mod: QPSK g: 25.000000 inlvl: 20% nac:  1F5 src:        0 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 25.000000 inlvl: 20% nac:  1F5 src:        0 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 25.000000 inlvl: 22% nac:  1F5 src:        0 tg:     0
Sync:  +P25p1     o:   24 mod: QPSK g: 25.000000 inlvl: 21% nac:  1F5 src:        0 tg:     0
Sync:  +P25p1     o:   24 mod: QPSK g: 25.000000 inlvl: 22% nac:  1F5 src:        0 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 38.783203 inlvl: 23% nac:  1F5 src:        0 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 27.538504 inlvl: 21% nac:  1F5 src:        0 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 22.825897 inlvl: 22% nac:  1F5 src:        0 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 22.825897 inlvl: 20% nac:  1F5 src:        0 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 22.825897 inlvl: 22% nac:  1F5 src:  4270002 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 18.995476 inlvl: 24% nac:  1F5 src:  4270002 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 16.667957 inlvl: 23% nac:  1F5 src:  4270002 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 16.497547 inlvl: 20% nac:  1F5 src:  4270002 tg:  7455
Sync:  +P25p1     o:   24 mod: QPSK g: 16.497547 inlvl: 20% nac:  1F5 src:  4270002 tg:  7455
```

Figura 3.25: Trama de P25 fase 1 descodificada

Como se observa en la figura previa se obtienen los datos de origen y destino de la transmisión, así como el grupo al que pertenece esta y la modulación usada.

Adicionalmente a los datos mostrados, obviamente, se descodifica el audio. Este puede ser enviado a una salida de audio para obtener el audio en tiempo real y adicionalmente puede guardarse en un archivo en formato WAV.

3.3.5. D-STAR

La interceptación de D-STAR es muy similar a la que se realiza con P25. Existen diversas aplicaciones para obtener el audio de las conversaciones y datos en el flujo de la transmisión.

Para la interceptación, aprovechando que ya se ha nombrado y explicado anteriormente, se puede hacer uso de DSD, el cual incluye la posibilidad de identificar y decodificar las tramas de D-STAR.

Con la opción -fd se indica que las tramas a decodificar sean D-STAR, por lo que en el momento de captar una transmisión esta será decodificada y se obtendrá el contenido en formato de audio.

Debido a que D-STAR permite el cifrado de las comunicaciones, si la transmisión interceptada hiciera uso de este, no sería posible la obtención del contenido.

```
Decoder options:
  -fa           Auto-detect frame type (default)
  -f1           Decode only P25 Phase 1
  -fd           Decode only D-STAR
  -fi           Decode only NXDN48* (6.25 kHz) / IDAS*
  -fn           Decode only NXDN96 (12.5 kHz)
  -fp           Decode only ProVoice*
  -fr           Decode only DMR/MOTOTRBO
  -fx           Decode only X2-TDMA
  -l            Disable DMR/MOTOTRBO and NXDN input filtering
  -ma           Auto-select modulation optimizations (default)
  -mc           Use only C4FM modulation optimizations
  -mg           Use only GFSK modulation optimizations
  -mq           Use only QPSK modulation optimizations
  -pu           Unmute Encrypted P25
  -u <num>      Unvoiced speech quality (default=3)
  -xx           Expect non-inverted X2-TDMA signal
  -xr           Expect inverted DMR/MOTOTRBO signal

  * denotes frame types that cannot be auto-detected.
```

Figura 3.26: Opciones de decodificación de DSD

3.3.6. DMR

Dadas las similitudes que comparte con D-STAR, no es de extrañar que haciendo uso también de DSD sea posible obtener el contenido de las tramas que hacen uso de esta tecnología.

Para poder realizar la decodificación y obtener los datos y el audio de las transmisiones es necesario hacer uso de la opción -fr. Al contrario que con la decodificación de D-STAR, hay otras opciones que afectan a la calidad y los resultados de los datos obtenidos en la decodificación. La opción -xr es usada para invertir la señal de DMR. En algunos casos es posible que el audio decodificado se escuche distorsionado, esto puede ser a causa de que la señal esté invertida, haciendo uso del parámetro indicado (-xr) el contenido debería inteligible.

3.3.7. GSM

Para poder interceptar el tráfico GSM es necesario encontrarse en el rango de cobertura de, al menos, una BTS y conocer la frecuencia exacta que está haciendo uso.

Para esto es posible usar la herramienta Kalibrate- RTL, como bien se ha indicado en el punto de reconocimiento correspondiente.

Una vez se identifica la frecuencia exacta esta puede interceptarse haciendo uso de las suite de herramientas GR-GSM, antes conocido como Airprobe. Este conjunto de herramientas proporciona una interfaz que hace de pasarela entre los datos recibidos por el SDR y programas de análisis de paquetes de red, como Wireshark.

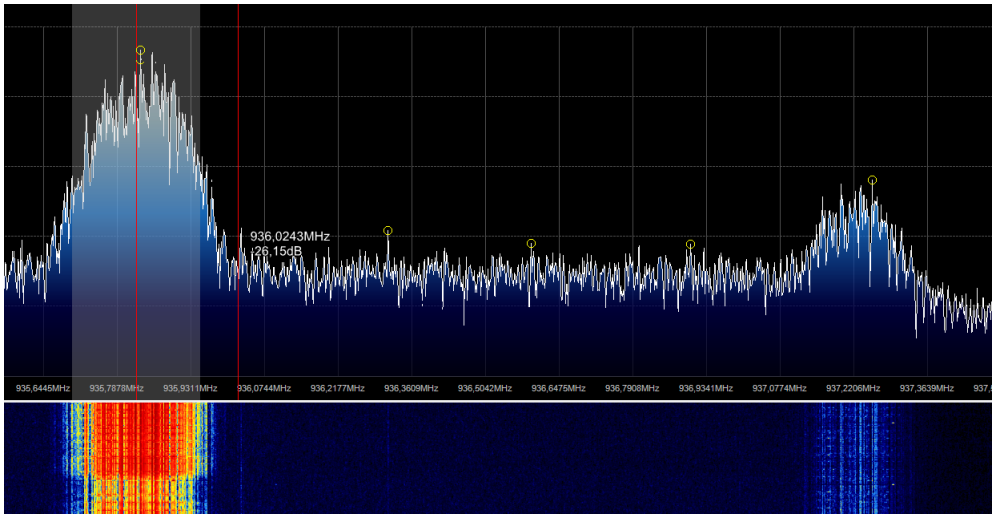

Figura 3.27: Inicio de la captura de GSM

Para ello hace uso de bloques de GNURadio diseñados especialmente para ello. Permitiendo la captura en tiempo real. Es decir, a través de una interfaz de usuario que es generada por el programa ejecutado en GNURadio, otorga al usuario la capacidad de realizar una variación de la frecuencia deseada para ser más preciso en la sintonización del canal GSM.

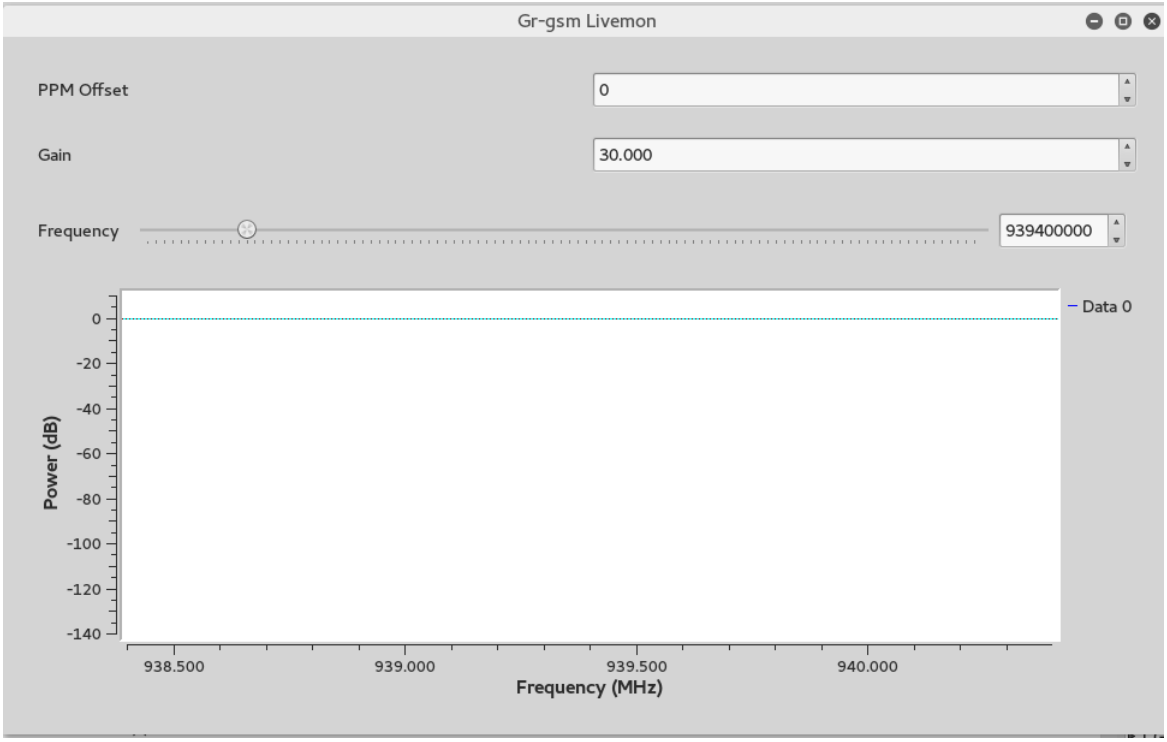

Figura 3.28: Interfaz de usuario del FLowgraph

En el momento que se consigue la sintonización de un canal GSM por la shell en la que se ejecuta el programa, como se muestra en la siguiente figura. Adicionalmente en la consola inferior de GNURadio se mostrará la trama de datos de GSM.

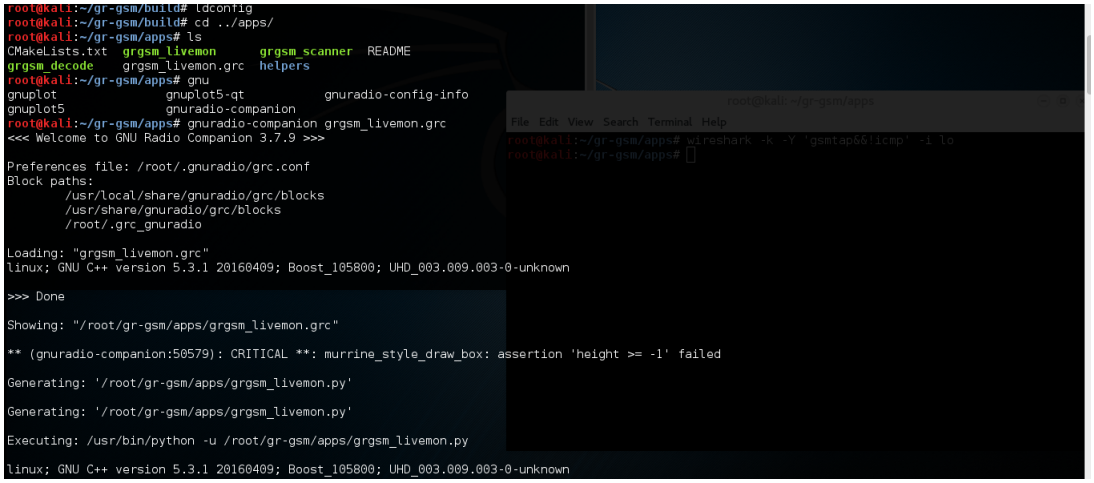

Figura 3.29: Trama de datos GSM capturada

Este proceso, se realiza con una instancia de Wireshark iniciada capturando paquetes en la interfaz *loopback*. En el momento que se comienza a realizar la captura de GSM los paquetes correspondientes se mostrarán en Wireshark.

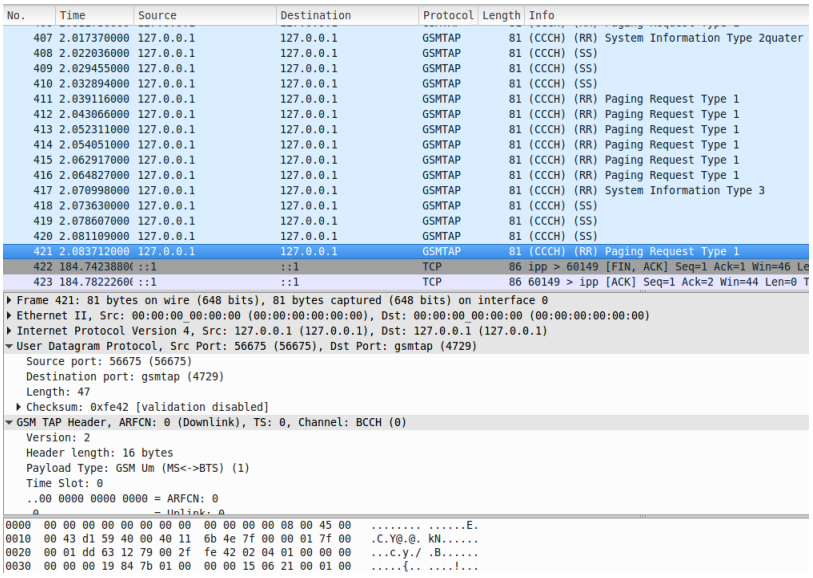

Figura 3.30: Visualización de los paquetes capturados en Wireshark

3.4 Inyección

3.4.1. Ataque de repetición

La forma más sencilla de realizar una inyección de datos en una transmisión es a través de la interceptación previa de contenido. Es decir, sería necesario obtener una trama de datos válida de ese protocolo para posteriormente reenviar lo capturado.

Es algo similar a la función que realizan los repetidores de radio, pero difiere de estos en que no tiene por qué realizarse en tiempo real.

Poniendo un ejemplo relativamente actual, es posible obtener los datos de las constelaciones de satélites GPS publicadas por la NASA para generar una señal GPS propia y válida en lo que respecta a los dispositivos que la reciban. De este modo sería posible variar la posición recibida, cambiar la fecha de un dispositivo o incluso generar una ruta que difiera de la real. Siendo los datos interpretados como legítimos para el dispositivo que los recibe.

Así mismo en transmisiones en las que se realicen comunicaciones por voz, es posible realizar una emisión de datos reales y válidos. Por ejemplo, el caso de los *walkie-talkie*.

Para obtener mejores resultados en este tipo de ataque se puede combinar con técnicas de *jamming* entre el emisor y receptor legítimos.

En el Anexo A se ejemplifica este tipo de ataque haciendo uso de la técnica conocida como MouseJack.

CAPÍTULO 4
Conclusión

Actualmente las telecomunicaciones inalámbricas son una gran parte de las comunicaciones que son realizadas en medios tanto profesionales como personales. Muchas de estas conteniendo información de carácter sensible que, teniendo la falsa creencia de que son seguras, "se lanzan al aire" con la seguridad de que alcancen su destino sin ser alteradas ni interceptadas. Esto como bien se ha explicado en el punto correspondiente a los antecedentes no es totalmente cierto.

Si bien es cierto que debido a la basta implantación de sistemas de radiofrecuencia existentes y a la variada implantación que hacen los diferentes fabricantes de estos, es virtualmente imposible conseguir información útil de todas las transmisiones de radio que cruzan el planeta diariamente. Sin embargo, es una realidad, que es posible obtener información de un tipo de transmisión en concreto, siempre que se encuentre dentro del alcance.

Teniendo en cuenta la gran cantidad de sistemas que hay actualmente, desde el punto de vista de la seguridad, el uso que más interés genera es el de la obtención de información. Debido a que actualmente, y en la mayoría de los casos, se hace uso de tecnologías ya asentadas y de las cuales existe suficiente información como para sacar provecho de sus deficiencias. Un claro ejemplo de esto son las transmisiones de los cuerpos del estado, que pueden interceptarse por hacer uso de TETRA.

Pese a que el mayor beneficio se centre en la obtención de información no hay que descartar la posibilidad de poder aprovechar vulnerabilidades de los diferentes protocolos y tecnologías para realizar modificaciones o accesos no legítimos a las infraestructuras que proporcionan la interfaz de comunicación. Para ello es necesario hacer un análisis exhaustivo acerca de cada una de las tecnologías que vayan a ser auditadas (en este documento se ha realizado una aproximación a unas pocas), para así mediante ingeniería inversa identificar las deficiencias de las cuales se puede sacar provecho.

Se concluye por tanto con lo siguiente, es necesario tratar a cada una de las tecnologías como si de un sistema independiente se tratase, del mismo modo que se hace con Bluetooth o WiFi. Analizando sus protocolos, tecnología base, modulaciones y herramientas, hardware y software, necesarias. No es posible, por tanto, establecer una metodología general que se adapte a todas las tecnologías de telecomunicación a través de radio, pero si establecer unas bases sobre las cuales desarrollar el proceso de auditoría de estas.

Bibliografía

[1] MouseJack (o por qué no usar ratones inálambricos). Consultado en https://www.securityartwork.es/2017/06/14/mousejack-no-usar-ratones-inalambricos/.

[2] RTL-SDR TUTORIAL: LISTENING TO TETRA RADIO CHANNELS Consultado en http://www.rtl-sdr.com/rtl-sdr-tutorial-listening-tetra-radio-channels/.

[3] RTL-SDR TUTORIAL: DECODING DIGITAL VOICE (P25, DMR, NXDN, D-STAR) WITH DSD Consultado en http://www.rtl-sdr.com/rtl-sdr-radio-scanner-tutorial-decoding-digital-voice-p25-with-dsd/.

[4] SIGFOX Consultado en http://www.sigidwiki.com/wiki/SIGFOX.

[5] RTL-SDR TUTORIAL: POCSAG PAGER DECODING Consultado en http://www.rtl-sdr.com/rtl-sdr-tutorial-pocsag-pager-decoding/.

[6] Disposición 4950 del BOE núm. 114 de 2014 Consultado en https://www.boe.es/boe/dias/2014/05/10/pdfs/BOE-A-2014-4950.pdf.

[7] MouseJack: Injecting keystrokes into wireless mice. Consultado en https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Marc-Newlin-MouseJack-Injecting-Keystrokes-Into-Wireless-Mice.pdf.

[8] Hacking the wireless world with software defined radio Consultado en https://www.blackhat.com/docs/asia-15/materials/asia-15-Seeber-Hacking-the-Wireless-World-With-Software-Defined-Radio-2.0.pdf.

[9] SNIFFING AND ANALYZING GSM SIGNALS WITH GR-GSM Consultado en http://www.rtl-sdr.com/sniffing-analyzing-gsm-signals-gr-gsm/.

[10] Decrypting GSM phone calls Consultado en https://srlabs.de/bites/decrypting-gsm/.

[11] LoRa Alliance Consultado en https://www.lora-alliance.org/.

[12] mousejack_transmit Consultado en https://github.com/iamckn/mousejack_transmit.

[13] nrfresearchfirmware Consultado en https://github.com/BastilleResearch/nrf-research-firmware/.

[14] mousejack Consultado en https://github.com/BastilleResearch/mousejack.

APÉNDICE A
Prueba de concepto MouseJack

En este anexo se muestra una prueba de concepto del ataque MouseJack. Haciendo uso de este tipo de ataque es posible realizar la repetición de transmisiones de radio, así como generar nuevos mensajes para hacerse pasar por un dispositivo legítimo.

A.1 Configuración

La configuración necesaria pasa por la instalación de un software modificado sobre un *dongle* usb con el chip nRF24LU1+.

En este caso se ha usado el dispositivo USB ideado para controlar el Dron CrazyFlie, ya que es facilmente modificable y dispone de un conector de antena externa para aumentar la recepción.

Figura A.1: Dispositivo usado

Esto es relativamente sencillo haciendo uso del firmware nrf-research-firmware y las herramientas desarrolladas por el propio equipo de Bastille.

A.2 Identificación

Haciendo uso del *scanner* es posible identificar si en las proximidades (dependiendo de la antena y entorno el rango de recepción varía) existe algún dispositivo que se corresponda con este tipo de comunicaciones, lo que no significa que sea vulnerable.

```
sudo ./nrf24-scanner.py -l
```

El parámetro -l se corresponde con el LNA, lo que es únicamente posible haciendo uso del Crazyflie Radio USB.

A.3 Interceptación

Durante las pruebas se ha identificado un dispositivo, cuya dirección (similar a la MAC) es "34:XX:XX:XX:07" (los valores intermedios han sido modificados por seguridad). El siguiente paso es capturar, que es lo que se envía, para ello se hace uso de nrf24-sniffer.py y se le indica la dirección a analizar.

```
sudo ./nrf24-sniffer.py -l -a 34:XX:XX:XX:07
```

El resultado obtenido por pantalla es similar al siguiente:

```
00:D3:B0:E2:E1:3C:0A:EF:1F:9B:85:CB:8A:D9:00:00:00:00:00:00:00:18
00:4F:00:00:55:00:00:00:00:5C
00:40:00:55:6B
00:4F:00:00:16:00:00:00:00:9B
00:D3:83:7C:EC:EF:54:1C:AE:F0:85:CB:8A:DA:00:00:00:00:00:00:00:91
00:4F:00:00:55:00:00:00:00:5C
00:4F:00:03:70:00:00:00:00:3E
00:40:03:70:4D
00:40:03:70:4D
00:40:03:70:4D
00:40:03:70:4D
00:40:03:70:4D
00:40:03:70:4D
00:40:03:70:4D
00:40:03:70:4D
00:40:03:70:4D
00:D3:C6:8E:BE:13:DE:CD:0F:79:85:CB:8A:DB:00:00:00:00:00:00:00:20
00:4F:00:00:55:00:00:00:00:5C
00:4F:00:00:16:00:00:00:00:9B
```

Los mensajes de mayor longitud se corresponden con pulsaciones de teclas, mientras que los de longitud intermedia y menor se corresoponden con mensajes de confirmación y *keepalive*, respectivamente.

A.4 Inyección

Es posible enviar "pulsaciones" de teclas, como si de un teclado real se tratase, al receptor del teclado/ratón. De este modo es posible preparar ataques de tipo HID, similar a los que se realizan con un Rubber Ducky, con la excepción de que es necesario tener un enlace establecido entre nuestro dispositivo emisor y el receptor.

Para ello, es necesario usar una versión modificada de las herramientas de Bastille, concretamente hay que hacer uso de la herramienta 'nrf24-replay.py' la cual permite enviar "pulsaciones" a la víctima. Codificando cada uno de los carácteres tal y como hace

el teclado, de ahí que sea necesario interceptar el tráfico de la misma marca de teclado. Dado ese caso, es posible generar una serie de ordenes que puedan descargar contenido malicioso en el equipo de la víctima.

```
sudo ./nrf24-replay.py -l -a 34:XX:XX:XX:07 -i keylogs/dropper.log
```

Donde en dropper.log se encuentran codificados los comandos para descargar contenido malicioso en el equipo de la víctima.