GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

EVALUACIÓN DE MECANISMOS DE CIBERSEGURIDAD EN EL SECTOR DEL AUTOMÓVIL

Autor: José Ramón Porro Nieves

Director: Gregorio López López

Co-Director: Roberto Gesteira Miñarro

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título Evaluación de mecanismos de ciberseguridad en el sector del automóvil en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el curso académico 2022/23 es de mi autoría, original e inédito y no ha sido presentado con anterioridad a otros efectos. El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido tomada de otros documentos está debidamente referenciada.

Fdo.: José Ramón Porro Nieves Fecha: 4 / 7 / 2023

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Gregorio López López Fecha: ……/ ……/ ……

EL CODIRECTOR DEL PROYECTO

GESTEIRA MIÑARRO ROBERTO - 48228840W

Firmado digitalmente por GESTEIRA MIÑARRO ROBERTO - 48228840W
Fecha: 2023.07.05 08:39:01 +02'00'

Fdo.: Roberto Gesteira Miñarro Fecha: ……/ ……/ ……

Trabajo Fin de Grado

Grado en Ingeniería en Tecnologías de Telecomunicación

Evaluación de mecanismos de ciberseguridad en el sector del automóvil

Autor:
José Ramón Porro Nieves

Directores:
Gregorio López López
Roberto Gesteira Miñarro

Madrid

Agradecimientos

A mi madre.

A mi padre y mi hermana por el apoyo incondicional que me han dado siempre.

A mis directores de proyecto, Gregorio López y Roberto Gesteira, por su dedicación y su dirección en el proceso de realización de este proyecto de investigación.

A mis amigos y mis compañeros por su apoyo y paciencia.

EVALUACIÓN DE MECANISMOS DE CIBERSEGURIDAD EN EL SECTOR DEL AUTOMÓVIL

Autor: Porro Nieves, José Ramón.
Director: López López, Gregorio.
Codirector: Gesteira Miñarro, Roberto
Entidad Colaboradora: ICAI – Universidad Pontificia Comillas

RESUMEN DEL PROYECTO

En este proyecto se presenta una metodología para el análisis de las comunicaciones entre vehículos y sus llaves mediante radiofrecuencia que permita evaluar el nivel de exposición y las vulnerabilidades de estos sistemas. Se ha realizado un análisis exhaustivo del sistema PKE de un vehículo y se ha analizado el sistema RKE de otro vehículo.

Palabras clave: Radiofrecuencia, ciberseguridad, vehículos.

1. Introducción

La ciberseguridad se podría definir como uno de los desafíos más importantes de la era digital. En el ámbito del automóvil, a medida que la electrónica se ha ido introduciendo en los vehículos, desde las primeras unidades electrónicas de control (ECU) hasta los más recientes sistemas de conducción autónoma, los vehículos más modernos han visto incrementadas las posibilidades de ser vulnerables a ataques e interferencias de terceros.

2. Definición del proyecto

Desde hace varios años se ha detectado que existe un grave problema de seguridad en los sistemas de apertura y cierre por control remoto en los automóviles actuales.

En el ámbito de la ciberseguridad, se pretende definir una metodología que ofrezca la posibilidad de evaluar el nivel de seguridad de los sistemas de apertura electrónica de los vehículos.

Por este motivo, este Trabajo Fin de Grado busca ofrecer una metodología de análisis de sistemas *keyless* que permita analizar, evaluar y comparar las tramas intercambiadas entre llaves electrónicas y vehículos por medio de radiofrecuencia, además de poder realizar pruebas de concepto basadas en ataques documentados en la literatura.

3. Descripción del sistema

La metodología desarrollada permite realizar capturas de las señales intercambiadas entre el mando o llave electrónica y el vehículo en cuestión utilizando herramientas SDR como HackRF One y GNU Radio Companion. Para el análisis de las señales capturadas se emplea el software libre inspectrum que permite decodificar las señales y obtener la trama binaria que contienen. Esto posibilita la identificación de la estructura de trama que permite el desarrollo de herramientas software de ataque dirigido.

4. Resultados

La metodología propuesta en este proyecto se ha puesto en práctica tanto en un sistema *keyless* como en un sistema de códigos evolutivos. En la tabla 1, se muestra un resumen de las características del vehículo A.

Tabla 1. Características del sistema del vehículo A

Modulación	2FSK Manchester
Comunicación	Bidireccional
Tasa de símbolo	2.6 kBd
Frecuencia de trabajo	838.3 MHz (UHF Llave -> Vehículo) 20 kHz (LF Vehículo -> Llave)
Tamaño de trama	234 bits
Tamaño de los datos	96 bits

La mayoría de los fabricantes utiliza modulaciones sencillas como 2FSK o ASK/OOK para la transmisión de datos entre el vehículo y llave. Esta transmisión se suele realizar en bandas no licenciadas como 433 MHz o 868 MHz en Europa y 315 MHz en América. En muchos casos se suele emplear codificación Manchester para transmitir información en UHF.

Los sistemas *keyless* denominados sistemas Passive Keyless Entry (PKE) suelen emplear una combinación de canales de transmisión, habitualmente hay un canal de baja frecuencia (LF) para la transmisión de información desde el coche hacia la llave inteligente, este canal de transmisión es de corto alcance y velocidad de transmisión reducida. Por otro lado, hay otro canal de comunicación en alta frecuencia (UHF) empleado para la transmisión de datos desde la llave hacia el vehículo.

El canal de transmisión en baja frecuencia además de hacer posible la comunicación entre vehículo y llave, también permite al vehículo determinar si la llave se encuentra cerca del vehículo o en su interior.

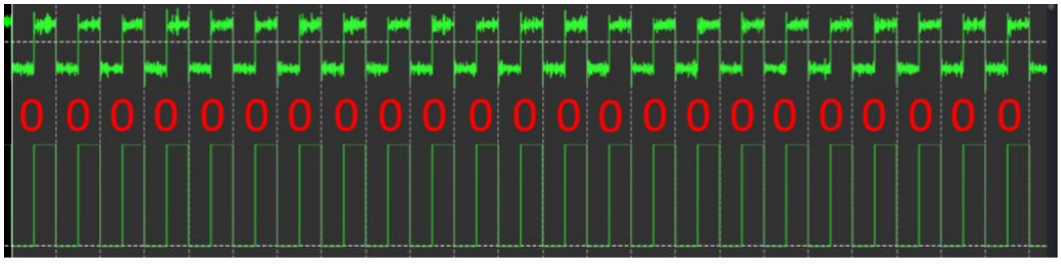


Fig. 1. Secuencia de sincronismo. Modulación 2FSK. Codificación Manchester.

En el sistema PKE analizado, el coche inicia la comunicación enviando una señal de activación por el canal de baja frecuencia a la llave que permanece en un modo de bajo consumo esperando esa señal. Cuando la llave recibe esa señal, esta se activa y transmite una respuesta por el canal UHF (868.3 MHz). En el caso analizado, se trata de una señal modulada en 2FSK con codificación Manchester compuesta por un preámbulo o secuencia

de sincronismo (ver Fig. 1) seguida de 96 bits de datos que contienen el ID de llave, un código de acción (abrir/cerrar el vehículo o la apertura del maletero), un código evolutivo y un *checksum* (ver Fig. 2).

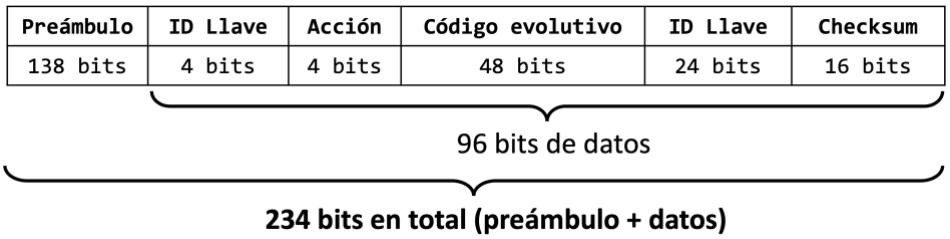


Fig. 2. Estructura de la trama transmitida

Gracias al análisis binario de las diferentes tramas se ha logrado identificar el ID de las llaves escaneadas y los códigos de acción asociados al bloqueo, desbloqueo de puertas y apertura del maletero. Esta identificación de la estructura de trama es muy útil para realizar posibles ataques de diccionario y determinar si el vehículo es vulnerable.

5. Conclusiones

Tras la finalización del proyecto y en base a los resultados obtenidos, se ha conseguido definir una metodología de análisis para comunicaciones de radiofrecuencia de sistemas RKE y sistemas *keyless* (PKE). También se han analizado las diferentes tipologías de sistemas PKE que suelen encontrar en los vehículos y se ha definido un procedimiento para su análisis exhaustivo (tanto a nivel *hardware* como a nivel de *software)* y su evaluación.

6. Referencias

[1] A.I. Alrabady y S.M. Mahmud. “Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs”. En: IEEE Transactions on Vehicular Technology 54.1 (2005), págs. 41-50. doi: 10.1109/TVT.2004.838829. https://ieeexplore.ieee.org/document/1386610

[2] EuroCybcar. Los vehículos deberán tener un certificado de ciberseguridad. Nueva normativa.: https://eurocybcar.com/wp-content/uploads/2021/02/EUROCYBCAR_INFORME_normativa_ONU-UNECE-WP29.pdf (visitado 12-11-2022)..

[3] Flavio D. Garcia et al. “Lock It and Still Lose It —on the (In)Security of Automotive Remote Keyless Entry Systems”. En: 25th USENIX Security Symposium (USENIX Security 16). Austin, TX: USENIX Association, ago. de 2016. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia

EVALUATION OF CYBERSECURITY MECHANISMS IN THE AUTOMOBILE SECTOR

Author: Porro Nieves, José Ramón.
Supervisor: López López, Gregorio.
Cosupervisor: Gesteira Miñarro, Roberto
Collaborating Entity: ICAI – Universidad Pontificia Comillas

ABSTRACT

This project presents a methodology for the analysis of communications between vehicles and their keys through radiofrequency that allows evaluating the level of exposure and the vulnerabilities of these systems. A thorough analysis of the PKE system of one vehicle has been carried out and the RKE system of another vehicle has been analyzed.

Keywords: Radiofrequency, cybersecurity, vehicles

1. Introduction

Cybersecurity could be defined as one of the most important challenges of the digital age. In the automotive field, as electronics have been introduced into vehicles, from the first electronic control units (ECUs) to the most recent autonomous driving systems, the most modern vehicles have seen an increased chance of being vulnerable. to third party attacks and interference.

2. Project defintion

For several years it has been detected that there is a serious security problem in the remote control opening and closing systems in current automobiles.

In the field of cybersecurity, it is intended to define a methodology that offers the possibility of evaluating the level of security of electronic vehicle entry systems.

For this reason, this Final Degree Project seeks to offer a keyless systems analysis methodology that allows the analysis, evaluation and comparison of the frames exchanged between electronic keys and vehicles by means of radio frequency, in addition to being able to carry out proofs of concept based on documented attacks in Literature.

3. System description

The developed methodology allows capturing the signals exchanged between the remote control or electronic key and the vehicle in question using SDR tools such as HackRF One and GNU Radio Companion. For the analysis of the captured signals, the free software inspectrum is used, which allows decoding the signals and obtaining the binary frame they contain. This makes it possible to identify the frame structure that allows the development of targeted attack software tools.

4. Results

The methodology proposed in this project has been put into practice both in a keyless system and in an evolutionary code system. Table 1 shows a summary of the characteristics of vehicle A.

5. *Table 2. Características del sistema del vehículo A*

Modulation	2FSK Manchester
Communication	Bidirectional
Baudrate	2.6 kBd
Frecuency	838.3 MHz (UHF Keyfob -> Car) 20 kHz (LF Car -> Keyfob)
Packet size	234 bits
Data size	96 bits

Most manufacturers use simple modulations such as 2FSK or ASK/OOK for data transmission between the vehicle and the key. This transmission is usually carried out in unlicensed bands such as 433 MHz or 868 MHz in Europe and 315 MHz in America. In many cases, Manchester coding is often used to transmit information in UHF.

The keyless systems also known as Passive Keyless Entry (PKE) systems usually use a combination of transmission channels, usually there is a low frequency (LF) channel for the transmission of information from the car to the smart key, this transmission channel is short range and high speed. reduced transmission. On the other hand, there is another high frecuency (UHF) communication channel used to transmit data from the key to the vehicle.

The low frequency transmission channel, in addition to making communication between the vehicle and the key possible, also allows the vehicle to determine if the key is near the vehicle or inside it.

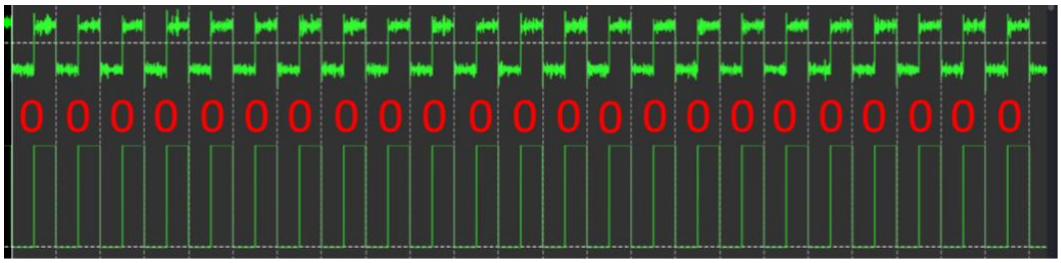


Fig. 3. Preamble. 2FSK Modulation. Manchester Encoding.

In the PKE system analyzed, the car initiates communication by sending an activation signal through the low frequency channel to the key, which remains in a low consumption mode waiting for that signal. When the key receives this signal, it is activated and transmits a response on the UHF channel (868.3 MHz). In the case analyzed, it is a 2FSK modulated signal with Manchester coding made up of a preamble or synchronization sequence (see Fig. 1) followed by 96 data bits containing the key ID, an action code (open/ closing the vehicle or opening the trunk), an evolutionary code and a checksum (see Fig. 2).

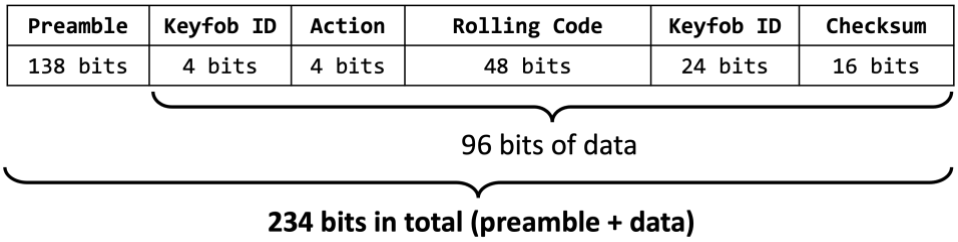


Fig. 4. Packet structure of the transmitted signal

Thanks to the binary analysis of the different frames, it has been possible to identify the ID of the scanned keys and the action codes associated with locking, unlocking doors and opening the trunk. This identification of the frame structure is very useful for performing possible dictionary attacks and determining if the vehicle is vulnerable.

6. Conclusions

After the completion of the project and based on the results obtained, it has been possible to define an analysis methodology for radiofrequency communications of RKE systems and keyless systems (PKE). The different types of PKE systems that are usually found in vehicles have also been analyzed and a procedure has been defined for their exhaustive analysis (both at the hardware and software level) and their evaluation.

7. References

[1] A.I. Alrabady y S.M. Mahmud. "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs". En: IEEE Transactions on Vehicular Technology 54.1 (2005), págs. 41-50. doi: 10.1109/TVT.2004.838829. https://ieeexplore.ieee.org/document/1386610

[2] EuroCybcar. Los vehículos deberán tener un certificado de ciberseguridad. Nueva normativa.: https://eurocybcar.com/wp-content/uploads/2021/02/EUROCYBCAR_INFORME_normativa_ONU-UNECE-WP29.pdf (visitado 12-11-2022)..

[3] Flavio D. Garcia et al. "Lock It and Still Lose It —on the (In)Security of Automotive Remote Keyless Entry Systems". En: 25th USENIX Security Symposium (USENIX Security 16). Austin, TX: USENIX Association, ago. de 2016. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia

Índice general

Índice de figuras

Índice de tablas

Listings

Glosario de abreviaturas

BLE Bluetooth Low Energy

CAN Controlled Area Network

LF Low Frecuency

MAC Media Access Control

OBD On-board diagnostics

PKE Passive Keyless Entry

RKE Remote Keyless Entry

RFID Radio Frequency Identification

RSSI Received Signal Strength Indicator

UHF Ultra High Frecuency

Capítulo 1

Introducción

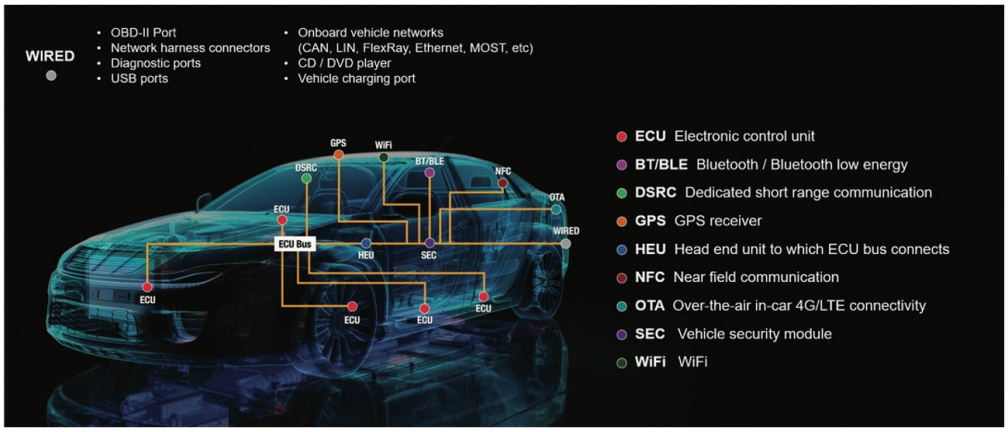


Figura 1.1: Esquema tecnologías automóvil [1]

La ciberseguridad se podría definir como uno de los desafíos más importantes de la era digital. En el ámbito del automóvil, a medida que la electrónica se ha ido introduciendo en los vehículos, desde las primeras unidades electrónicas de control (ECU) hasta los más recientes sistemas de conducción autónoma, los vehículos más modernos han visto incrementadas las posibilidades de ser vulnerables a ataques e interferencias de terceros. En la Fig. 1.1 se muestran algunas de las tecnologías que incorpora un automóvil moderno, estas tecnologías constituyen diferentes vectores de ataque y suponen un riesgo si no se verifica que sean seguras.

La ciberseguridad del vehículo es un concepto muy amplio, puede englobar desde ataques a través del puerto OBD (On-board diagnostics), ataques al bus CAN

(Controlled Area Network) del vehículo o incluso el control del vehículo de forma remota a través de la red móvil de datos. Sin embargo, este proyecto de fin de grado se va a centrar en el ámbito de las comunicaciones por radiofrecuencia, su funcionamiento y posibles vulnerabilidades.

Desde hace varios años se ha detectado que existe un grave problema de seguridad en los sistemas de apertura y cierre por control remoto en los automóviles actuales. Un delincuente podría abrir con facilidad los coches de otros usuarios en el aparcamiento de por ejemplo un centro comercial. En las últimas décadas se han desarrollado herramientas de escaneo de radiofrecuencia portátiles que permitirían capturar el código que envía el transmisor del mando o llave y una vez capturado el código, este podría ser utilizado para ser retransmitido con el objetivo de abrir ese coche. Aunque esto no es tan sencillo pues muchos modelos modernos incorporan soluciones que mitigan parcialmente este problema mediante el uso de los códigos evolutivos.

Tras la adopción por parte de la industria del automóvil de la solución de los códigos evolutivos, han surgido nuevas formas de entender la apertura del vehículo como por ejemplo los sistemas de acceso *keyless* o la apertura a través de un *smartphone* que constituyen un nuevo vector de ataque para los ciberdelincuentes.

Ante esta situación, es necesario disponer de metodologías para analizar la seguridad de estos sistemas e investigar cuál es su grado de seguridad. Por eso, este Trabajo Fin de Grado busca ofrecer una metodología de análisis de sistemas *keyless* que permite analizar, evaluar y comparar las tramas intercambiadas entre llaves electrónicas y vehículos por medio de radiofrecuencia, además de poder realizar pruebas de concepto basadas en ataques documentados en la literatura.

Tal y como se ha indicado al comienzo, este Trabajo Fin de Grado se centra en ataques de radiofrecuencia (RF) pero va más allá de los conocidos ataques dado que se realiza un análisis digital binario de las tramas transmitidas y de los protocolos implantados en los diferentes vehículos.

Capítulo 2

Definición del trabajo

2.1. Justificación

La justificación de este proyecto es llevar a cabo un análisis de la ciberseguridad de los vehículos particulares en el ámbito de la radiofrecuencia.

Este proyecto de investigación puede resultar de gran utilidad a fabricantes de vehículos, empresas aseguradoras entre otros y en definitiva a los propios usuarios de los vehículos, ya que aporta información acerca del estado de la seguridad de los sistemas de radiofrecuencia, apertura y arranque de distintos vehículos.

Por otro lado, se tiene constancia de problemas de ciberseguridad en los automóviles desde 2012, la UNECE (Comisión Económica de las Naciones Unidas para Europa) desarrolló la normativa de seguridad UNECE/R155, que entró en vigor en enero de 2021, y establece los requisitos mínimos de ciberseguridad que debe cumplir un vehículo, afectando a coches, furgonetas, autocaravanas, camiones, remolques y autobuses que se homologuen desde julio de 2022, y a todos los que se comercialicen desde julio de 2024 en la Unión Europea y en todos los territorios adheridos hasta ahora a la normativa: Rusia, Japón, Corea del Sur, Sudáfrica y Australia. [2]

2.2. Objetivos del proyecto

Los objetivos de este proyecto son varios:

- Analizar el estado de la técnica: Investigar el funcionamiento de los sistemas PKE y posibles vulnerabilidades.
- Analizar el funcionamiento de sistemas *keyless* en diferentes vehículos.
- Realizar ataques como prueba de concepto de lo analizado.

2.3. Metodología y plan de trabajo

Se ha decidido seguir el siguiente plan de trabajo. En primer lugar, se realizará un estudio de la técnica en el que se buscará comprender las diferentes tecnologías existentes y en desarrollo. Una vez finalizada la parte de investigación, se realizan capturas de las señales de radiofrecuencia emitidas por la llave y el vehículo. Posteriormente, se analizarán las diferentes señales capturadas y se identificarán sus características como tipo de modulación de la señal, estructura identificada en el código, etc. Por último, se realizará un estudio de los resultados obtenidos con el objetivo de realizar pruebas de ataque o emulación de llave como prueba de concepto.

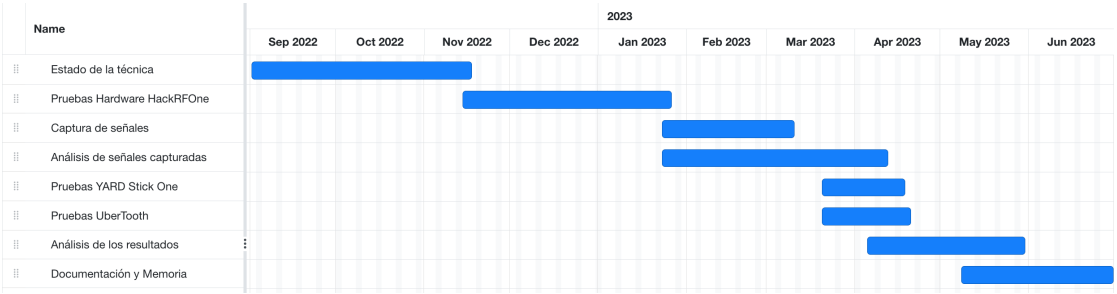


Figura 2.1: Cronograma del proyecto

Capítulo 3

Estado del arte

3.1. Introducción

Los sistemas de apertura a distancia son un componente fundamental en cualquier vehículo actual. La comunicación por ondas de radio ha sido hasta ahora el método preferido para la apertura y control a distancia de los vehículos, aunque recientemente se ha comenzado a observar en el mercado otros métodos para la apertura y arranque como por ejemplo el uso de tarjetas RFID [1] o llaves inteligentes, un smartphone con tecnologías Wi-Fi o Bluetooth [3].

Los primeros sistemas de cierre centralizado o apertura sin llave (es decir, que permitían la apertura del vehículo sin emplear la clásica llave o espadín, sino accionando el botón de un mando) se remontan a los años 90 y funcionaban con sistemas de código fijo. El nivel de seguridad de estos sistemas solía ser mínimo, quizás en aquel momento era suficiente pero a medida que la tecnología sigue avanzando, resulta más sencillo el acceso a equipos de radiofrecuencia así como la captura y reproducción de la señales, haciéndolos completamente vulnerables. Posteriormente, como solución al dilema de los sistemas de código único surgieron los sistemas de código variable o códigos evolutivos.

Paralelamente alrededor del año 2000, se comenzó a instalar en coches de alta gama un sistema comercialmente denominado como acceso "confort" o sistemas *keyless*. Este sistema permitía el acceso y arranque del mismo sin tener que accionar el

[1] Radio Frequency Identification

mando, simplemente era necesario llevarlo en el bolsillo o maleta de forma que permaneciese cerca del vehículo. De ahora en adelante, nos referiremos a estos como sistemas PKE (Passive Keyless Entry).

3.2. Sistemas RKE

Un sistema RKE (Remote Keyless Entry) es cualquier sistema de cierre centralizado por control remoto.

Curiosamente, el primer RKE en un vehículo de serie no se implementó en un modelo de clase superior, sino en el Renault Fuego de 1982. Pero a partir de comienzos de los años 90, la tecnología empezó a ser usada por otros fabricantes. En los primeros diseños de sistemas RKE, un transmisor de corto alcance con un radio de cinco hasta diez metros enviaba un comando sin codificar de apertura o de cierre al receptor del vehículo; en Norteamérica generalmente a 315 MHz, en Europa y Asia a 433,92 MHz. La recepción de la señal se confirmaba de forma óptica a través de los intermitentes o de forma acústica con la bocina. [4]

Hay diferentes tipos de sistemas que se describen a continuación.

3.2.1. Sistemas de código fijo

Tal y como se ha mencionado en la introducción de este capítulo, los sistemas de código fijo (*fixed-code*) supusieron el nacimiento de los sistemas de cierre centralizado con control remoto. Utilizaban un único código por eso se denomina de código fijo.

El protocolo era muy sencillo y la comunicación era unidireccional. El coche tenía un transceptor que permanecía a la espera de la señal del mando. Cuando se accionaba el boton de apertura, el mando transmitía una señal con el código único, el coche la recibía y si el código coincidía con el esperado se accionaba la apertura del vehículo y en caso contrario no se realizaba ninguna acción (ver Fig. 3.1).

Estos sistemas han quedado completamente en desuso en los vehículos actuales y es común encontrarlos en algunas puertas y mecanismos automáticos. Es un sistema vulnerable y resulta muy fácil replicar la señal tantas veces como se quiera. No

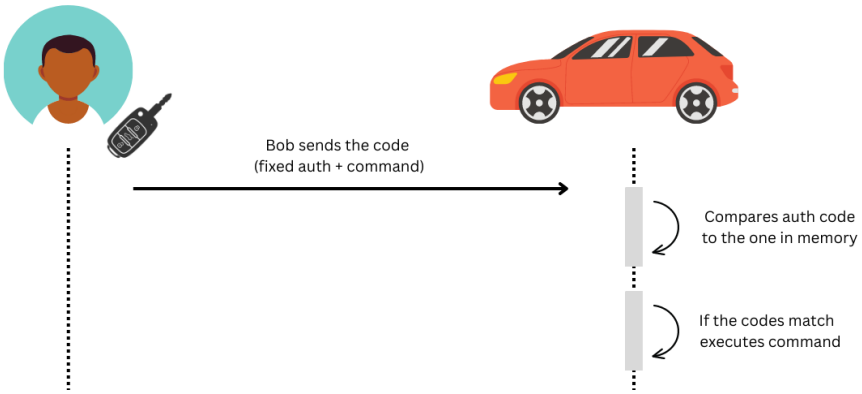


Figura 3.1: Sistemas de código fijo [5]

Figura 3.2: Esquema generación código evolutivo [6]

sería necesario ni decodificar la señal, se podría capturar la señal en bruto con una SDR como HackRF One y reproducir ese fichero en bruto para simular la transmisión de llave o mando legítimo.

3.2.2. Sistemas de código evolutivo

Como respuesta a la escasa seguridad de los sistemas de código único surgieron los códigos evolutivos.

Al emplear un sistema de códigos evolutivos, se genera un código nuevo para cada transmisión utilizando criptografía simétrica o generadores de números pseudo-aleatorios. De esta forma, los códigos previamente transmitidos dejan de ser válidos, por lo que no sería posible capturar un código y reutilizarlo si el vehículo lo ha recibido. El problema de esta solución es que no protege de ataques *jam and re-*

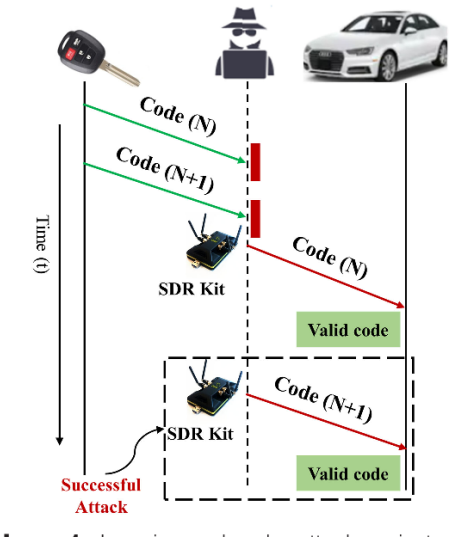


Figura 3.3: Diagrama de ataque de *replay* con *jamming* [6]

play [6]. Un ataque de *jam and replay* tiene dos fases, en primer lugar, el atacante genera una señal de interferencia para que el vehículo no pueda recibir la señal que envía el mando. El atacante captura la primera señal enviada (N). Como el coche no ha realizado ninguna acción, el usuario vuelve a presionar el botón del mando. El atacante captura la segunda señal (N+1) y transmite al coche la primera señal que capturó (N) de forma que el vehículo recibirá la señal y actuará normalmente y el atacante tiene un código (N+1) que es válido dado que es el siguiente código en la lista. Este proceso se puede observar ilustrado en la Fig. 3.3.

En la Fig. 3.4 se puede observar un diagrama simplificado del funcionamiento de un generador de códigos aleatorios. En primer lugar, se define S como una clave secreta compartida por el vehículo y la llave y N como el contador que tambien comparten. Cuando se acciona el mando, se genera un código utilizando la clave secreta S y el contador N. Acto seguido se incrementa N y se envía el código junto con otra información al vehículo. El vehículo genera el código esperado de la misma forma que lo ha hecho la llave y si ambos coinciden se ejecuta la acción y en caso contrario no se realiza nada. Por último, se incrementa el contador N del vehículo. Cabe mencionar que el contador no tiene del vehículo y la llave no tienen que coincidir exactamente, hay una ventana de varios códigos que se pueden utilizar por lo que es posible cierto desfase entre los contadores. Sin embargo, si se acciona el suficiente nùmero de veces el mando fuera del alcance de radio del vehículo la diferencia entre el contador se la llave y el vehículo se puede hacer tan grande que dejará funcionar pues se habrá superado el umbral de la ventana de códigos

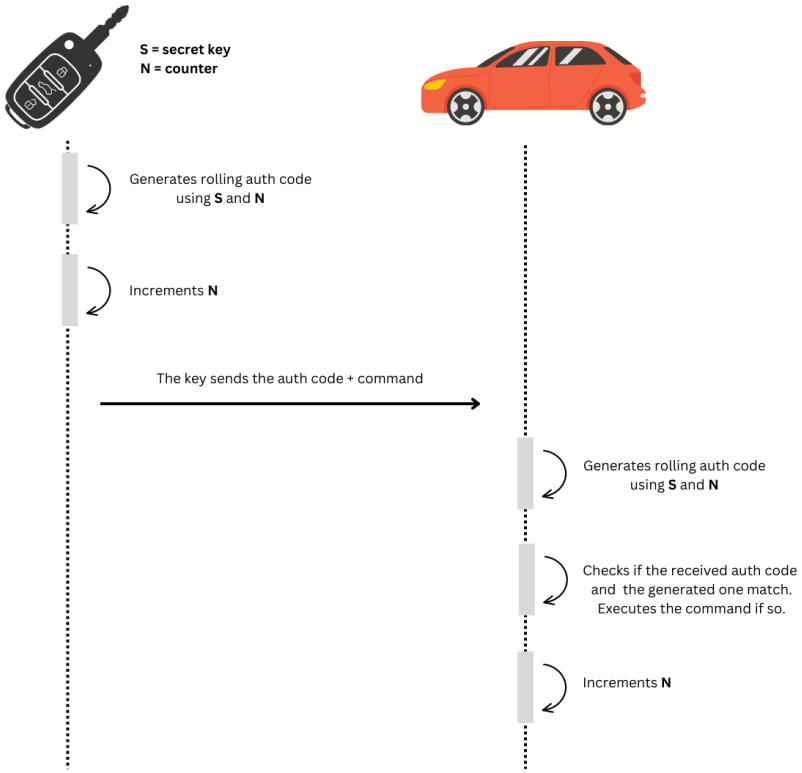


Figura 3.4: Sistemas de código evolutivo [5]

válidos.

Se debe tener en cuenta que este sistema tiene el problema de que se puede perder la sincronización del contador entre la llave y el vehículo por lo que el sistema dejaría de funcionar pues los códigos generados no coincidirían con los códigos esperados por el vehículo. Para solucionar este problema, se tendría que incorporar un procedimiento o protocolo de resincronización entre el mando y el vehículo.

Algoritmos de generación de códigos evolutivos como Keeloq y Hitag2 en los que se basa la seguridad de muchísimos sistemas RKE han sido desmontados y expuestos por investigadores de ciberseguridad [7]. Pero aunque estos sistemas puedan eventualmente ser vulnerables, comparados con los sistemas de código único fijo, ofrecen un alto grado de seguridad.

3.3. Sistemas desafío-respuesta

En este tipo de despliegue, el vehículo envía un desafío o prueba a la llave que consiste en un número aleatorio. Acto seguido, la llave encripta o procesa ese código y lo transmite de vuelta al vehículo. El vehículo compara la respuesta recibida con el resultado del algoritmo y si coincide, el vehículo se abre o arranca en el caso de un inmovilizador. Esta técnica es ampliamente utilizada en sistemas PKE conocidos comercialmente como *keyless entry*.

Los métodos de autenticación (código evolutivo y desafio-respuesta) tienen varias aplicaciones, las principales son en sistemas RKE, RKI (Remote Keyless Ignition) que es el sistema encargado de permitir o no el arranque del motor del vehículo similar al caso de los inmovilizadores.

3.4. Sistemas PKE

En los automóviles más recientes es muy común encontrar sistemas comercialmente denominados *"keyless"* o de acceso "confort", en los que se produce una comunicación bidireccional entre el vehículo y la llave. Este sistema permite la apertura y arranque del vehículo sin realizar interacción alguna con la llave, siendo necesario que se encuentre cerca del vehículo y permitiendo por ejemplo la apertura del vehículo con el simple movimiento de pasar el pie por debajo de un sensor estratégicamente colocado en la zona inferior de portón trasero.

Los sistemas PKE son más complejos que los sistemas RKE pues utilizan varios canales de comunicación de forma simultánea. En la Fig. 3.5 se representa los componentes de un sistema PKE tanto en el lado del vehículo (izquierda) como en el lado del mando (derecha). Se puede observar que la llave incorpora antenas para varias bandas de frecuencia (UHF y LF) y todo está gobernado por un microcontrolador. En el lado del vehículo, llama la atención que el sistema de baja frecuencia cuenta con una estación base dedicada exclusivamente a la gestión de este banda, lo cual tiene sentido debido al gran número de antenas que incorpora un vehículo de estas características.

En la Fig. 3.6 se puede observar que un automóvil con sistema PKE cuenta con varias antenas repartidas por todo el vehículo, algunas están posicionadas en el interior y otras en lugares como las manetas de las puertas o el maletero lugares

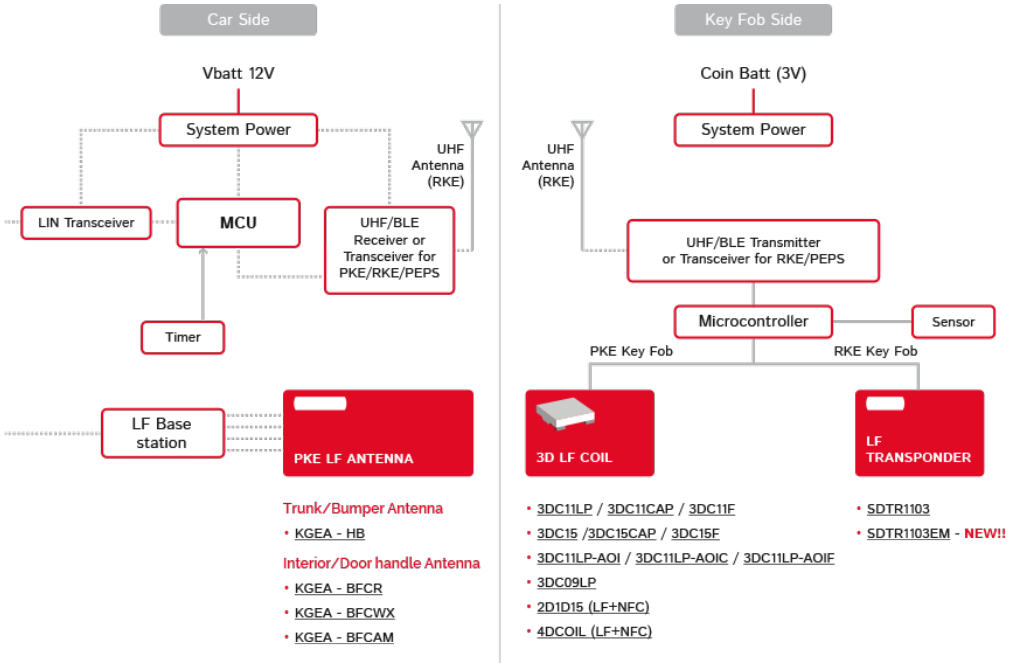


Figura 3.5: Esquema integral sistema PKE [8]

donde también hay incoporados sensores que detectan cuando el usuario va a abrir alguna de las puertas. Es importante que el protocolo de un sistema PKE sea rápido de forma que se asegure de que las puertas sean desbloqueadas antes de que la maneta haga su recorrido completo para que no se produzcan un bloqueo en el sistema mecánico de apertura [6].

La mayoría de sistemas PKE cuentan con una serie de antenas de tipo "loop" de baja frecuencia para determinar si la llave se encuentra cerca o dentro del vehículo. Sin embargo, hay otras tecnologías alternativas sobre las que se está investigando. Por un lado, se encuentra BLE.

BLE (Bluetooth Low Energy) es una tecnología que deriva del Bluetooth clásico. Esta tecnología ha sido implantada por algunos fabricantes de vehículos como por ejemplo Tesla. Es una alternativa a los sistemas *keyless* basados en antenas de baja frecuencia. Es una gran alternativa debido a su bajo consumo energético [9]. El problema es que su seguridad depende de parámetros Bluetooth como el RSSI (Received Signal Strength Indicator) o direcciones MAC, los cuales son inseguros tal y como se sugiere en [10] y [9].

También hay algunos estudios que presentan sistemas basados en ondas sonoras

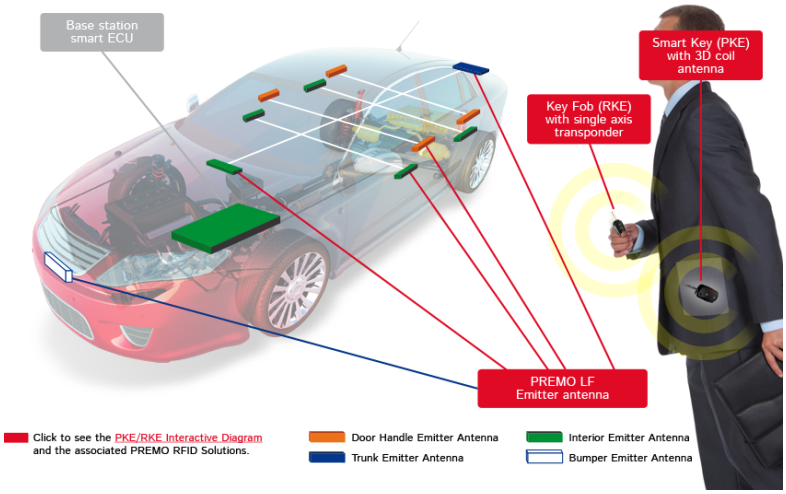


Figura 3.6: Diagrama de localización de las antenas en un vehículo con sistema PKE [8]

como forma de detectar la proximidad de la llave al vehículo como solución al problemático ataque de relay del que sufren los sistemas PKE clásicos [11].

3.5. Tipos de ataque

Se distinguen tres tipos de sistemas: unidireccional, bidireccional y pasivo. Los más implementados son el bidireccional y pasivo. En los sistemas pasivos también conocidos como PKE (Passive Keyless Entry) el proceso comienza cuando el usuario interacciona con el coche por ejemplo colocando la mano sobre la maneta de la puerta, en ese momento el coche envía una señal (solicitud). Si el mando se encuentra dentro del rango de cobertura del vehículo, el mando recibe la solicitud y envía una respuesta. Esa respiesta suele estar compuesta por el código evolutivo, un identificador de llave y un código de acción que puede ser por ejemplo abrir, cerrar o la apertura del maletero. El vehículo recibe la respuesta del mando y valida el código recibido. Si el código es legítimo y no ha sido recibido previamente, el vehículo se abre y se finaliza el proceso. [12].

3.5.1. Ataque de relay

Los métodos para iniciar el protocolo de llaves keyless PKE varían mucho entre fabricantes [3]. La gran mayoría de ellos son vulnerables a ataques de relay, también conocidos como proxy. Este ataque consiste en capturar la señal que emite la llave y transferirla al vehículo empleando un repetidor para lo cual se necesitarían dos atacantes, uno localizado cerca del vehículo y otro cerca de la llave (ver Fig. 3.7. Para evitar este ataque se han planteado soluciones utilizando timestamping [6]. Utilizando timestamping se busca detectar si la señal está siendo repetida, pues

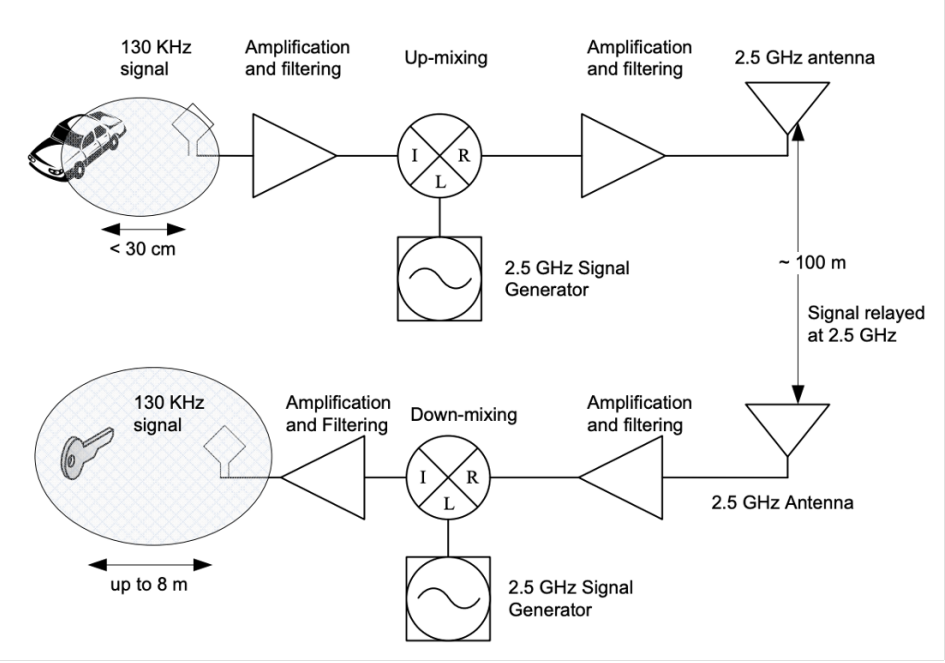


Figura 3.7: Diagrama relay attack

se introduce un delay al realizar este ataque debido al retardo introducido por el hardware utilizado y el procesado de la señal que en determinados casos puede ser necesario. Sin embargo, esto provoca que los sistemas tanto de la llave/mando como del vehículo sean más complejos y por lo tanto tengan un coste superior al de los sistemas tradicionales.

3.5.2. Ataque de replay

Este ataque es muy sencillo de realizar en un sistema de código fijo. Primero, se capturaría el código cuando el usuario accione el mando y como en estos sistemas siempre se envía el mismo codigo, se podría transmitir tantas veces como se quiera para abrir el vehículo.

Los automóviles actuales cuentan con sistemas de códigos evolutivos por lo que sería necesario que el algoritmo criptográfico estuviese comprometido como es el caso de KeeLoq2 [3] o introducir una señal de interferencia de forma que el vehículo no reciba la señal del mando y por lo tanto no descarte esos códigos. Este último ataque se conoce como ataque de *jam and replay* o ataque *rolljam*.

3.5.3. Ataque de diccionario

Otro ataque posible en determinados modelos es el ataque de diccionario también denominado de fuerza bruta. Este ataque consiste en tomar varias muestras de la señal transmitida por el mando, acto seguido se trata de identificar la estructura de la trama para identificar las diferentes partes de la señal y de esta forma diseñar una herramienta que pruebe un diccionario de códigos aleatorios [6]. El riesgo de este ataque es que el vehículo podría detectar que se está realizando este ataque y bloquearse para evitarlo [3].

Capítulo 4

Recursos

En este capítulo se detallan las herramientas hardware y software que se han empleado para la realización de este proyecto.

4.1. *Hardware*

Como herramientas hardware, se ha utilizado HackRF One, YARD Stick One y Ubertooth. Todos ellos diseñados por la firma Great Scott Gadgets.

HackRF One (ver Fig. 4.1 es un transceptor half-duplex que opera en el rango de 1 MHz a 6 GHz con hasta 20MHz de ancho de banda. Además, se trata de un

Figura 4.1: HackRF One. Hardware SDR.

Figura 4.2: YARD Stick One. Hardware.

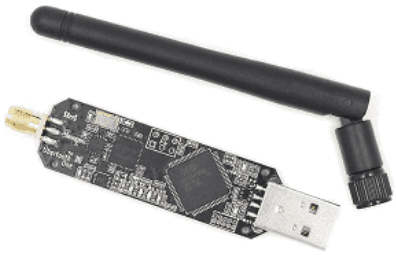


Figura 4.3: Ubertooth One. Hardware.

dispositivo open-source [13]. Este equipo se ha utilizado con la antena ANT500, se trata de una antena telescópica diseñada para operar de 75 MHz a 1 GHz y su longitud es configurable desde 20 cm hasta 88 cm [14].

YARDStickOne (ver Fig. 4.2, también es un transceptor half-duplex que opera en las frecuencias 300-348 MHz, 391-464 MHz y 798-928 MHz. Con este dispositivo es posible modular señales ASK/OOK, GFSK, 2FSK, 4FSK y bitrates de hasta 500 kbps [15].

Ubertooth (ver Fig. 4.3 es un receptor Bluetooth avanzado, que ofrece capacidades más allá de las de los adaptadores tradicionales, lo que permite que se use como una plataforma de rastreo y monitoreo de señales BT. Ninguno de los vehículos analizados contaba con la tecnología BLE o Bluetooth para la apertura o arranque

del vehículo. Por lo tanto, no se ha llegado a utilizar esta herramienta pero puede ser de gran interés como recurso para futuros desarrollos del proyecto.

4.2. *Software*

En cuanto a *software*, se ha utilizado GNU Radio, GQRX, inspectrum y rfcat. Son programas que funcionan en entornos Linux, para la realización de este proyecto se utilizará la distribución Kali Linux.

GNU Radio [16] es una herramienta de desarrollo libre y abierta que provee bloques de procesamiento de señal para implementar sistemas de radio definida por software (SDR). Se utilizará con HackRF One principalmente para la captura y reproducción de señales (ataques replay, relay, etc).

GQRX es un receptor radio definido por software que funciona con GNU Radio y el kit de herramientas Qt GUI. Puede procesar datos I / Q de muchos tipos de dispositivos de entrada. Se utilizará como analizador de espectro y para identificar la frecuencia de trabajo de las comunicaciones.

inspectrum es una herramienta para analizar las señales capturadas, obtener sus características e incluso decodificar una señal como bits.

rfcat es una librería de Python empleada para trabajar con el YARD Stick One ya sea empleando una consola o un script de Python.

Capítulo 5

Pruebas realizadas

En este capítulo se detalla la metodología que se ha seguido para el análisis de los vehículos.

5.1. Metodología de análisis

Se ha desarrollado una metodología para analizar el funcionamiento del sistema de cierre y apertura de vehículos que incorporan tanto sistemas RKE como sistemas PKE.

En primer lugar, será necesario identificar la frecuencia de trabajo de los equipos. Tipicamente se utilizan bandas no licenciadas como son 433 MHz y 868 MHz en Europa y 315 MHz en América. En algunos mandos viene indicada la frecuencia de trabajo del equipo como se puede observar en el ejemplo de la Fig. 5.4.

Si no aparece identificada la frecuencia de trabajo, normalmente se incluye el FCC ID u otro código de algún organismo de homologación. El FCC ID es número de identificación de la Comisión Federal de Comunicaciones que se puede encontrar en muchas piezas de hardware. A través de este código es posible acceder a una ficha en la que se indican las frecuencias de trabajo del equipo en cuestión y otra información de interés.

Si aún así no es posible encontrar esa información, los más sencillo es realizar un

escaneo de las bandas no licenciadas accionando el botón del mando en búsqueda de la señal tal y como se puede ver en la Fig. 5.1. Para ello se puede utilizar GQRX y una SDR como HackRF One.

También se puede abrir el mando para ver sus componentes y así tratar de identificar antenas de LF o UHF y otros componentes que pueden dar pistas sobre el funcionamiento del equipo.

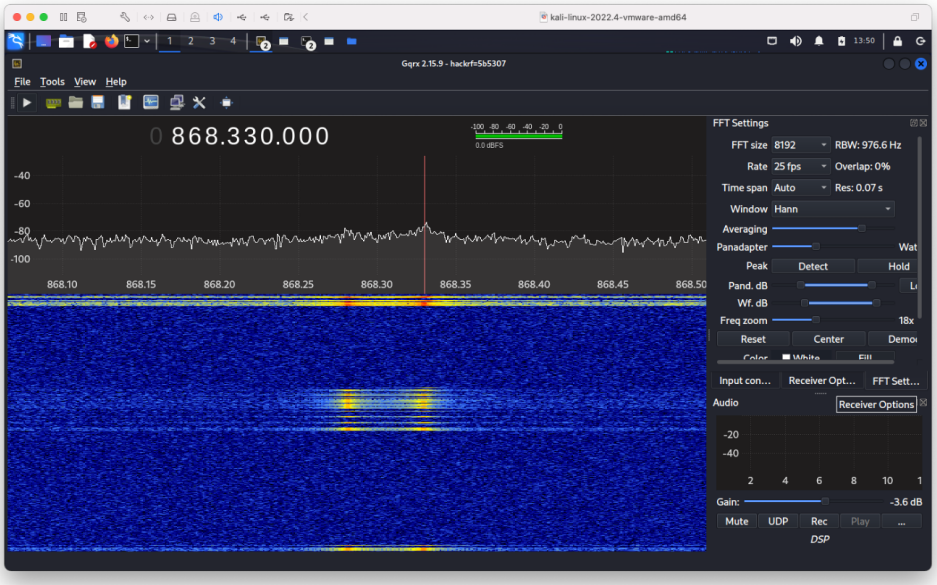


Figura 5.1: Interfaz GQRX. Señal 2FSK.

Una vez conocidas las frecuencias de trabajo, se procede a identificar qué tipo de sistema pasivo (PKES) incorpora el vehículo. Para ello, primero se escanea con un analizador de espectro (GQRX) si el vehículo envía una señal de activación de forma periódica. La mayoría de sistemas PKES se puede englobar en dos tipos, en uno el transpondedor del vehículo envía una señal periódica para comprobar si el mando se encuentra dentro del rango de cobertura y por lo tanto cerca del vehículo de forma que cuando el mando recibe esa señal, el mando se activa y responde. Otro tipo de PKES muy extendido es el que se activa cuando el usuario toca la maneta del coche, en este caso el vehículo solo envía la señal de activación cuando el usuario interacciona con el coche ya sea tirando de la maneta de alguna puerta o pulsando el botón de apertura del maletero. Esta señal de activación suele ser de baja frecuencia (LF) o 2.4 GHz.

En caso de no observar ninguna señal, se deberá accionar la manilla de la puerta

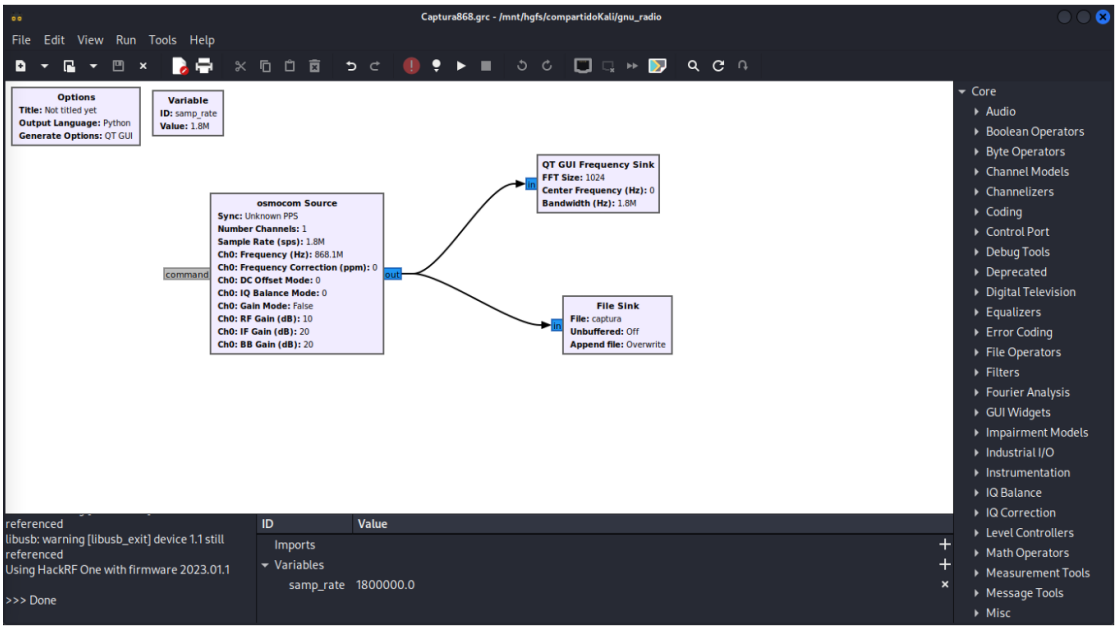


Figura 5.2: Interfaz GNU Radio. Diagrama de captura de señales.

del vehículo y se observará el intercambio de señales entre el vehículo y el mando. Debido a las limitaciones del equipo del que se disponía para la realización de este proyecto no es posible capturar las señales de activación de baja frecuencia pero normalmente la respuesta del mando se envía a través del canal de UHF por lo que la respuesta del mando sí se puede capturar y analizar.

Con la ayuda de GNU Radio Companion se captura esa señal y se analiza la trama con inspectrum. Una vez cargada la señal en inspectrum se puede identificar el tipo de modulación que típicamente es 2FSK con codificación Manchester o ASK/OOK. También se han encontrado determinados modelos en los que la frecuencia de transmisión va alternando entre dos frecuencias de transmisión cada vez que se accionaba el mando, posiblemente para dificultar la realización de un ataque de *replay*.

Una vez conocidas las características de tipo de modulación, frecuencia de trabajo, etc, se puede comenzar a realizar capturas de las señales utilizando GNU Radio (ver Fig. 5.2) y procesar esas capturas utilizando el software inspectrum que permite decodificar de forma semiautomática (utilizando cursores para definir cada símbolo) señales con modulación 2FSK y ASK/OOK.

5.2. Vehículo A

El vehículo A cuenta con dos métodos de apertura. Por un lado, se puede abrir accionando el botón de desbloquear de la llave actuando como un mando de coche tradicional. Por otro lado, el vehículo está equipado con un sistema de acceso *keyless* por lo que simplemente con llevar la llave en el bolsillo y tirar de la maneta de la puerta el vehículo se desbloqueará automáticamente.

Encontrar la frecuencia de trabajo del sistema RKE fue sencillo dado que venía impresa en la llave del vehículo tal y como se puede ver en la Fig. 5.4. Una vez conocida la frecuencia del equipo (868 MHz), se realizó un escaneo de la señal utilizando GQRX (ver Fig. 5.1). Se puede ver en la captura de pantalla que se trata de modulación 2FSK centrada en 868.3 MHz.

También cabe destacar que inicialmente se sospechó que podía estar transmitiendo el vehículo hacia la llave en el canal de UHF. Al realizar las mediciones, el vehículo y la llave estaban muy cerca del receptor HackRF One, por lo tanto no sería posible distinguir si la transmisión la está realizando el mando o el vehículo. Para descartar esto, se emplearon dos HackRFOne una situada cerca del vehículo y otra cercana a la llave lo más alejada posible del vehículo pero siendo posible la apertura remota del mismo. De esta forma, en base en los niveles de potencia observados en cada equipo, la conclusión fue que en canal de UHF solo transmite la llave y el vehículo solo transmite en LF.

Tras observar el espectro utilizando GQRX en diferentes situaciones: estado de reposo con el vehículo cerrado, estado de reposo con el vehículo abierto, apertura pulsando el botón (RKE), apertura automática al tirar de la maneta de la puerta (PKE) y otras situaciones se ha determinado que la llave actúa de forma idéntica en el canal de UHF (868.3 MHz) cuando se emplea el sistema RKE o PKE, lo que cambia es el método de activación de la llave. En un caso se presiona el botón de desbloquear de la propia y llave. En el otro caso, se introduce la mano en la maneta, esto es detectado por un sensor y el vehículo emite una señal de baja frecuencia y corto alcance para comunicar a la llave que se active (ver Fig.5.3). Las características de modulación de está señal se desconocen pues no se disponía de los recursos hardware para capturar señales de baja frecuencia. Sin embargo, se sabe que se encuentra alrededor de la banda de 20 kHz porque se ha observado que el mando incorpora una antena LF (ver Fig. 5.5) o bobina modelo Premo SMD 3D Coil Low profile SDC11LP-A-2000J cuya ficha técnica se puede ver en el anexo C y está diseñada para funcionar alrededor de esa frecuencia.

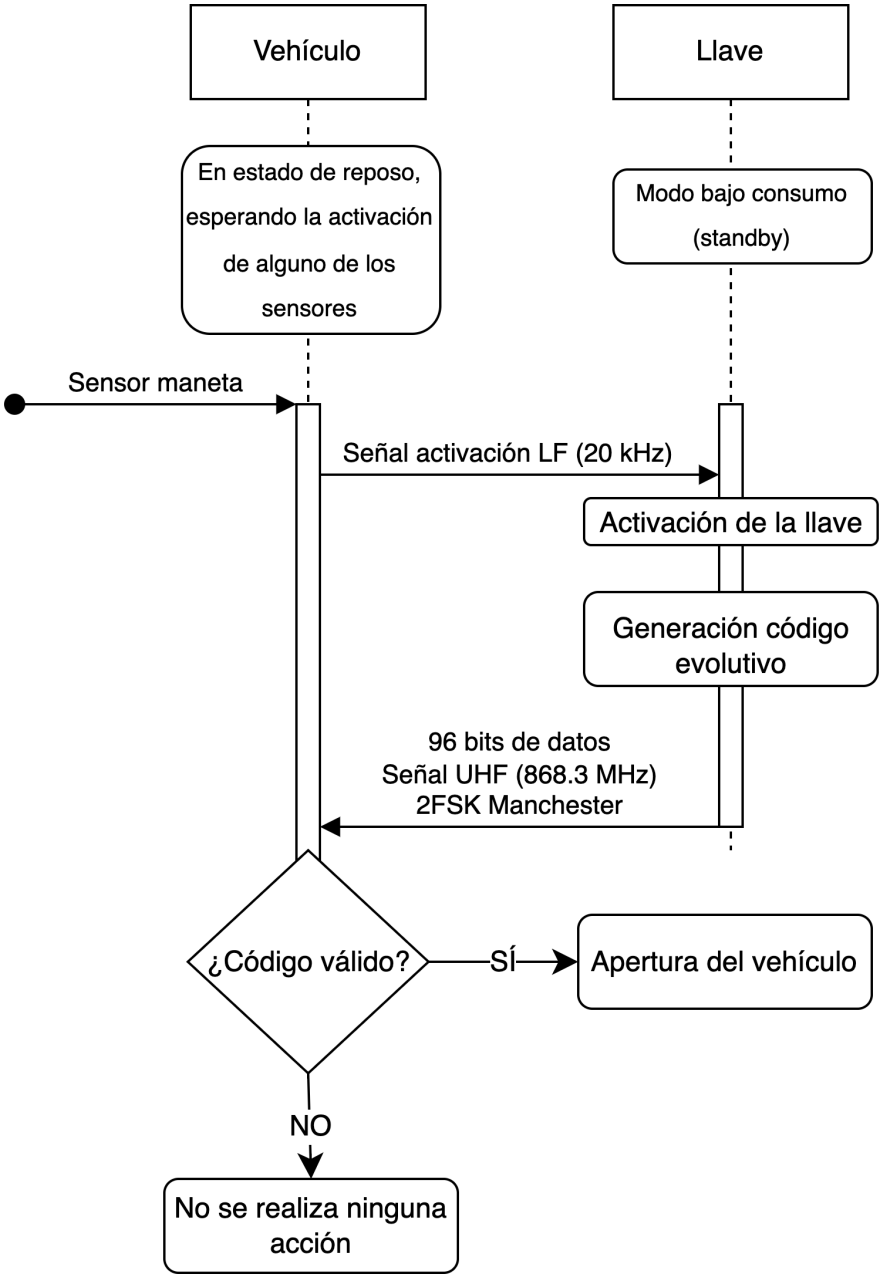


Figura 5.3: Diagrama de secuencia del protocolo PKE del vehículo A.

Si fuese posible capturar esa señal y reproducirla, se podría solicitar a la llave del vehículo de forma remota aunque a corta distancia, varios códigos de apertura válidos. Todo depende del tipo de señal que transmita por el canal de LF, si la señal es un código fijo sería bastante inseguro pues se podría realizar el ataque previamente descrito. Lo más probable es que se trate de un sistema *challenge-response* o desafío-respuesta (ver sección 3.3).

Figura 5.4: Detalle de impresión de la frecuencia de trabajo en el mando del automóvil A

Una vez conocidos los parámetros de frecuencia y modulación, se captura la señal utilizando el software GNU Radio utilizando un diagrama como el de la figura 5.2 y ajustando la variable `samp_rate` (*sample rate* o frecuencia de muestreo) a 1.8 MHz que es suficiente para capturar lo que se necesita y no genera ficheros excesivamente grandes, también se configura `Ch0: Frecuency (Hz)` a 868.1 MHz para evitar que la componente contínua que introduce HackRF One se superponga con la señal que se desea capturar.

Para analizar la señal capturada, se utiliza el software inspectrum. Para abrir el software y cargar la señal capturada se utiliza el comando:

`inspectrum <nombre_fichero>`.

Ajustando los niveles de *power max* y *power min* del espectrograma finalmente se obtiene una representación de la señal en tiempo y frecuencia (ver Fig. 5.6).

Para decodificar la señal en bits primero es necesario añadir cursores y ajustarlos al periodo de símbolo. Una vez añadidos los cursores (en total 468 símbolos) e indicada la frecuencia de muestreo (1.8 MHz), el software calcula el número de símbolos por segundo o *symbol rate* de 2.6 kBd. El software inspectrum no incorpora la funcionalidad de decodificar Manchester por lo que será necesario decodificar primero la señal en bruto como si fuese 2FSK sin Manchester y posteriormente realizar una operación de decodificación.

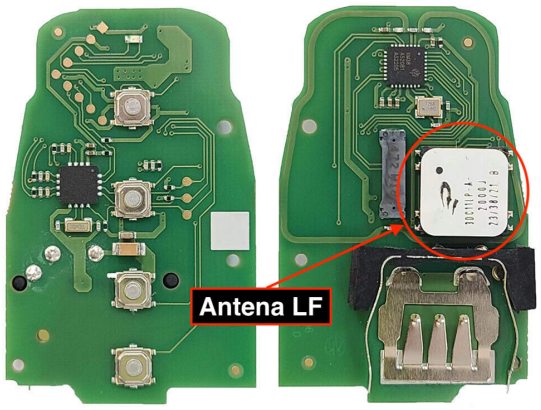


Figura 5.5: Interior del mando del vehículo A. Antena LF.

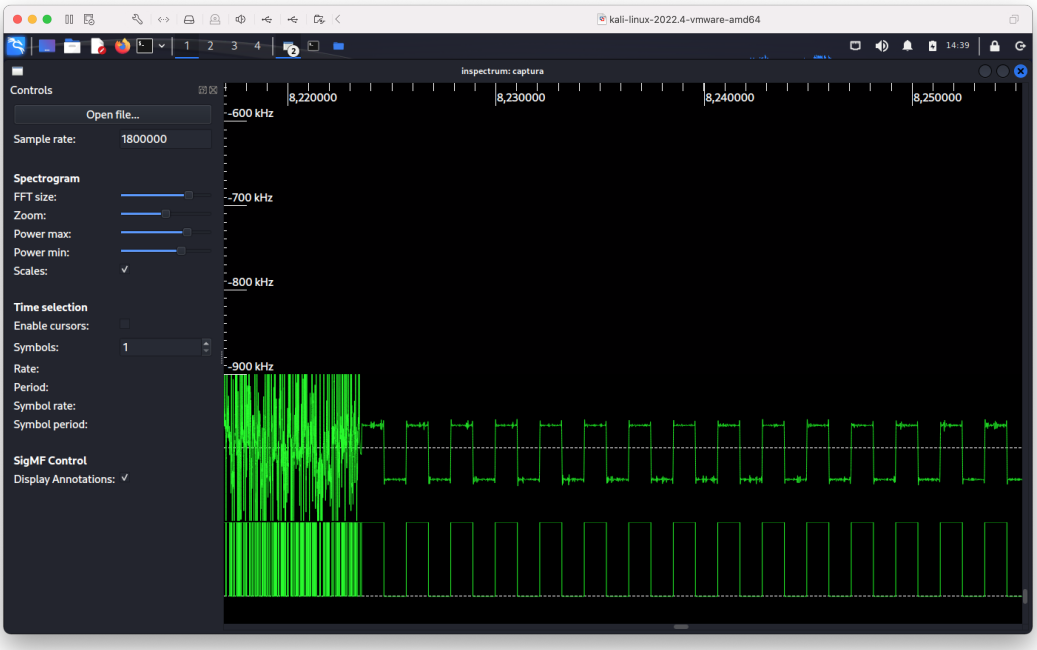


Figura 5.6: Captura de pantalla inspectrum (1)

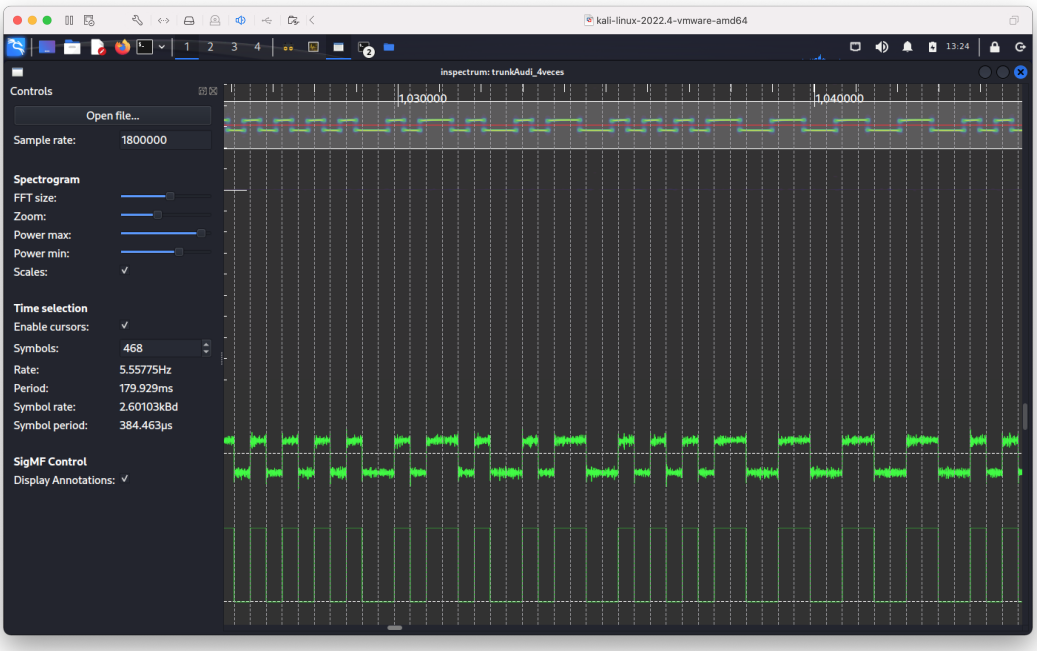


Figura 5.7: Captura de pantalla inspectrum (2)

En la figura 5.8 se puede ver el comienzo de la señal capturada llamado preámbulo o secuencia de sincronismo. Se han colocado los cursores ajustándose a los flancos de subida y de bajada, los cuales representan el verdadero símbolo a decodificar. Cabe recordar que el procedimiento descrito anteriormente se realiza porque inspectrum no soporta Manchester. En este trabajo de fin de grado se ha tomado el modelo de codificación Manchester propuesto por G. E. Thomas por lo que el flanco se subida representa un 0 y el de bajada un 1 (ver Fig. 5.9).

5.3. Vehículo B

Para identificar la frecuencia del vehículo B se realizó un escaneo por la bandas de frecuencia de 433 MHz y 868 MHz, observándose la señal transmitida por el mando en la banda de 433 MHz. Se observa que la señal está compuesta por una sola componente en la frecuencia 433.9 MHz. Para este vehículo se siguió un procedimiento muy similar al del vehículo A por lo que se realizará una descripción

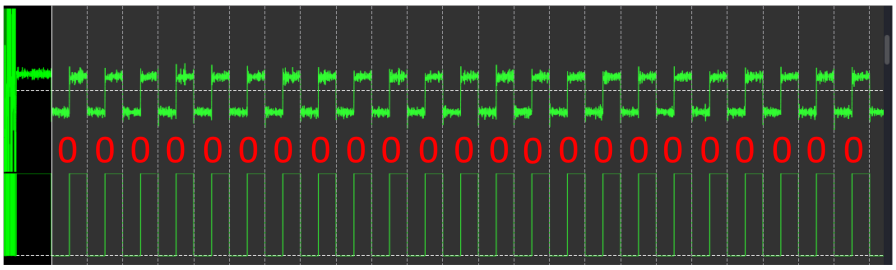


Figura 5.8: Vehículo A. Preámbulo. Modulación 2FSK. Codificación Manchester

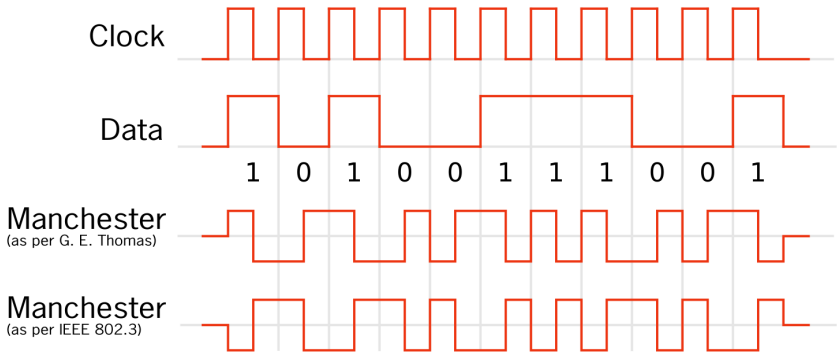


Figura 5.9: Codificación Manchester [17]

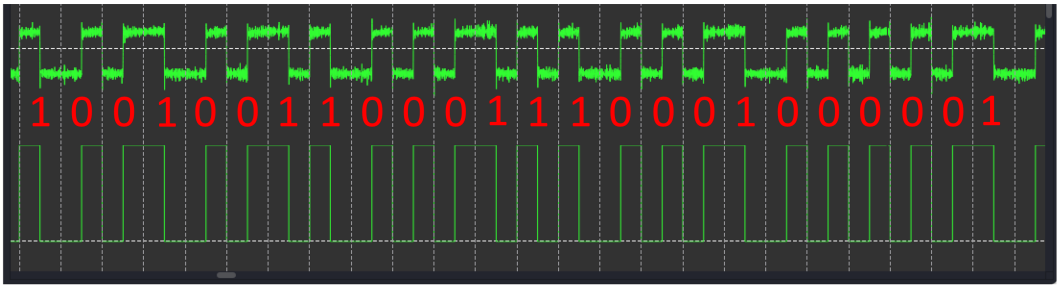


Figura 5.10: Vehículo A. Trama capturada. Codificación Manchester. Captura de pantalla del software inspectrum

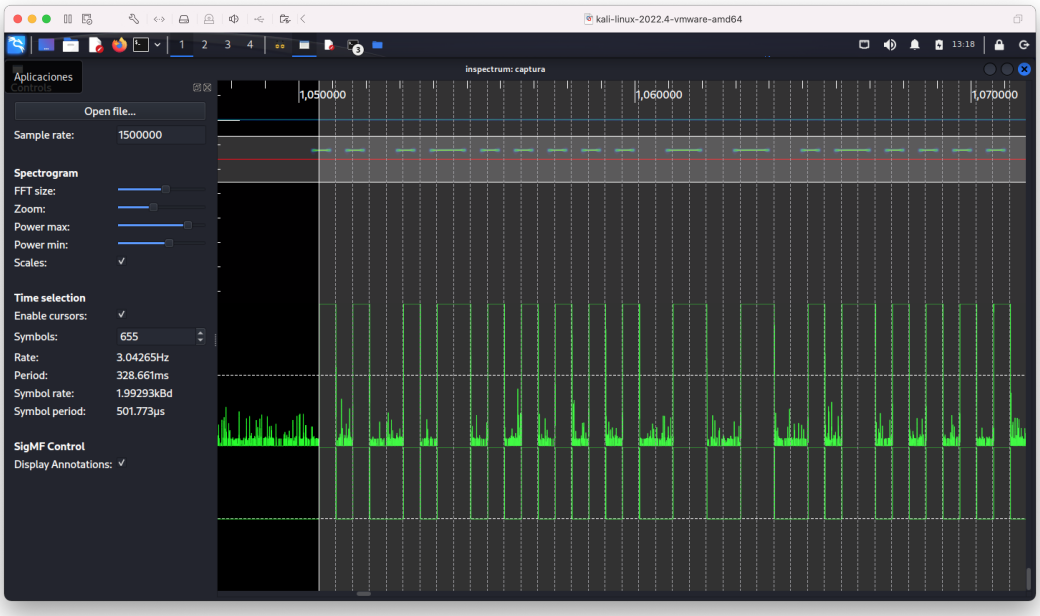


Figura 5.11: Vehículo B. Trama capturada. Modulación ASK/OOK. Captura de pantalla del software inspectrum

más resumida pues ya se ha explicado antes cómo se realiza.

Una vez identificada la frecuencia, realizó la captura de señales con GNU Radio y posterior decodificación con inspectrum. En este caso, la modulación utilizada es ASK/OOK (ver Fig.5.11).

La trama decodificada muestra un código de longitud 128 bits que se envía 5 veces repetido cada vez que se pulsa el botón de la llave.

Capítulo 6

Análisis de los resultados

En este capítulo se realiza una descripción detallada de los resultados obtenidos siguiendo la metodología descrita previamente.

6.1. Resultados vehículo A

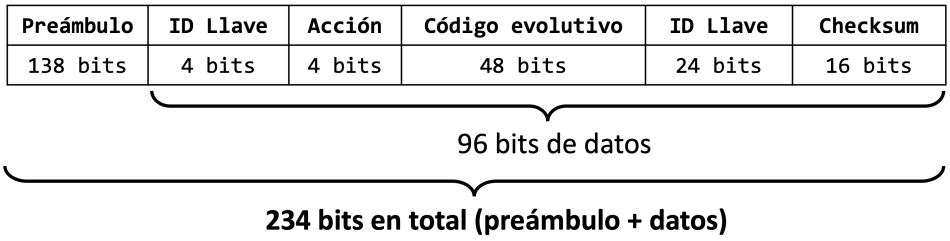
Tabla 6.1: Características del vehículo A.

Modulación	2FSK Manchester
Comunicación	Bidireccional
Baudrate	2.6 kBd
Frecuencia de trabajo	868.3 MHz (UHF Llave ->Vehículo) 20 kHz (LF Vehículo ->Llave)
Tamaño de trama	234 bits
Tamaño de los datos	96 bits

El vehículo A es un coche del año 2018, se ha analizado la comunicación de dos llaves. Esto ha facilitado la tarea de detectar patrones en las tramas de datos dado que hay una parte del código que permanecía fija en todas las señales de una determinada llave y cambiaban al escanear las señales de la segunda. Esto se puede observar comparando las tablas 6.4 (códigos de apertura capturados), 6.3 (códigos de cierre capturados) y 6.5 (códigos de apertura del maletero capturados).

El protocolo PKE que incorpora este vehículo funciona de la siguiente manera, el mando permanece en un modo de bajo consumo a la espera de una señal de activación por parte del coche. Esta señal de activación es de baja frecuencia y se encuentra alrededor de 20 kHz porque se ha observado que el mando incorpora una antena LF (ver Fig. 5.5) o bobina modelo Premo SMD 3D Coil Low profile SDC11LP-A-2000J cuya ficha técnica se encuentra en el Anexo C y está diseñada para funcionar alrededor de esa frecuencia. Se muestra un diagrama de secuencia del protocolo PKE en la Fig. 5.3 del capítulo 5.

Tabla 6.2: Vehiculo A. Estructura de trama.



Tras analizar varios códigos capturados de cada una de las acciones posibles (apertura, cierre y apertura del maletero) y comparando los códigos de las dos llaves ha sido posible identificar la estructura de trama (ver Fig. 6.2).

Esta identificación de la estructura de trama es muy útil para realizar posibles ataques de diccionario y determinar si el vehículo es vulnerable. Por último, cabe destacar que se ha realizado un ataque de *replay* al vehículo con éxito, utilizando el transmisor del YARD Stick One.

Tabla 6.3: Vehículo A. Códigos de apertura capturados.

Acción: LOCK	ID Llave	Acción	Código evolutivo	ID Llave	Checksum
Llave 1	1f	5	256d4e5713df	fffe64	ab34
	1f	5	2f0eed1261fe	fffe64	a8a3
	1f	5	b61bf4b6e6b4	fffe64	a51a
Llave 2	1e	5	0cec88573d96	fffff5	49d5
	1e	5	c2b690dda6cb	fffff5	467e
	1e	5	68ef801aca9a	fffff5	437a

Tabla 6.4: Vehículo A. Códigos de cierre capturados.

Acción: UNLOCK	ID Llave	Acción	Código evolutivo	ID Llave	Checksum
Llave 1	1f	7	0c791006bc07	fffe64	6f2f
	1f	7	84364099f94e	fffe64	6ca8
	1f	7	3792793fe1a8	fffe64	69d5
Llave 2	1e	7	9f168e7c34a5	fffff5	34b0
	1e	7	570b10900df2	fffff5	3116
	1e	7	fd98b36933f9	fffff5	2eef

Tabla 6.5: Vehículo A. Códigos de apertura del maletero (*trunk*) capturados.

Acción: TRUNK	ID Llave	Acción	Código evolutivo	ID Llave	Checksum
Llave 1	1f	6	9035ac98e20a	fffe64	2a80
	1f	6	a9b61cdf10cc	fffe64	27be
	1f	6	dfb144359d0f	fffe64	243a
Llave 2	1e	6	86d3aa016fe9	fffff5	1f5e
	1e	6	b1fd5a263d8a	fffff5	1cf4
	1e	6	0fc63f515938	fffff5	19f2

6.2. Resultados vehículo B

Tabla 6.6: Características del vehículo B.

Modulación	ASK/OOK
Comunicación	Unidireccional
Baudrate	2 kBd
Frecuencia de trabajo	433.9 MHz
Tamaño de trama	128 bits (x5)
Tamaño de los datos	128 bits

Tras analizar las tramas enviadas por la llave del vehículo B, no ha sido posible inferir cuál es la estructura de la trama pues no se ha observado un patrón en los códigos ni ningún otro tipo de relación.

A continuación, se muestran una batería de códigos capturados para las operaciones de apertura y cierre del vehículo.

```
LOCK (cierre)
================================
52d55332d54b4ccad54ccb2b3332acad
a5aa669a55a566969aa9a65a66656a65
52d52d54b52cd2aaacb4b2b2b332d553
4b554b4d2d4b4cb52b2b52cccccb4b4a

UNLOCK (apertura)
================================
25aaa5a696a5a65a9595a9666665a5a5
80826969aa9a99a6a5a995a6666595a5
25aa999a5a55aa59aa55596a6665556a
a5aa569a9696a99659695a69666556a5
```

Tal y como se puede ver, a priori no se identifica ninguna relación entre las tramas. Posiblemente, la totalidad de la trama está generado por un generador de códigos aleatorios, no existe una gestión de identificador de llave, sino que llave y vehículo comparten una semilla y contador. Pero por ejemplo en caso de pérdida de una llave no sería posible discriminar por llave para eliminarla del sistema, sería necesario reprogramar el sistema completo.

Aunque no se haya detectado la estructura de trama, como prueba de concepto, se

ha realizado un ataque de replay con éxito, consiguiéndose la apertura del vehículo utilizando el transmisor YARD Stick One. De forma que queda demostrado que los códigos capturados son codigos válidos y no se han producido errores en la captura y decodificación de los mismos.

Capítulo 7

Conclusiones y trabajos futuros

En este capítulo se sintetizan las conclusiones más importantes de este trabajo de fin de grado.

7.1. Conclusiones y principales resultados

En primer lugar, cabe mencionar que se han cubierto los tres objetivos iniciales del proyecto.

- Se ha realizado un análisis del estado del arte y se han identificado el funcionamiento de los diferentes tipos de sistemas de apertura remota así como de los ataques de radiofrecuencia documentados.

- Se ha desarrollado una metodología para el tratamiento y análisis de señales y más concretamente de sistemas pasivos (PKES) para poder evaluar la seguridad de los protocolos de comunicación implementados por los fabricantes de vehículos.

- Se han realizado ataques pasivos como prueba de concepto, verificando así la validez de los datos analizados.

Por otro lado, se ha redactado un manual sobre el uso de la librería `rfcat` que puede de gran utilidad para futuros desarrollos de software de ciberseguridad en

el ámbito de la radiofrecuencia.

Finalmente, se ha analizado con gran detalle el sistema *keyless* del vehículo A y se ha inferido la estructura de trama del mismo a través de un exhaustivo análisis de varias señales recopiladas.

7.2. Trabajos futuros

Una vez terminado el presente Trabajo Fin de Grado, surgen nuevas vertientes para continuar con la investigación de los sistemas de apertura y cierre de vehículos. Se pueden considerar los siguientes proyectos:

- Capturar y analizar las señales de activación de baja frecuencia (LF) propias de los sistemas *keyless* (PKE) e inmovilizadores de vehículos. Para analizar estas señales sería necesario utilizar el equipo adecuado y antenas de baja frecuencia.

- Continuar con el análisis de protocolos *keyless*. Aunque en este proyecto se ha realizado el análisis de un sistema *keyless* sería conveniente analizar más vehículos pues estos protocolos son muy variados y complejos.

- Analizar el algoritmo de generación de códigos evolutivos. El algoritmo utilizado para generar los distintos códigos evolutivos tiene un mecanismo de resincronización para el caso en el que un mando pierda la sincronización.

- Investigar el uso de tecnologías Bluetooth y BLE. Existen varios modelos comerciales que ya incorporan esta tecnología para la apertura y cierre de vehículos. Sería interesante evaluar la seguridad de estos sistemas menos comunes.

- Investigar otros vectores de ataque en vehículos. Tal y como se ha indicado en la introducción de este Trabajo Fin de Grado, existen otros vectores de ataque como por ejemplo, el puerto OBD del vehículo que sería interesante analizar.

Bibliografía

[1] L. Teschler. *Safety and cyber security for the connected car*. URL: https://www.microcontrollertips.com/safety-and-cyber-security-for-the-connected-car-faq/.

[2] EuroCybcar. *Los vehículos deberán tener un certificado de ciberseguridad. Nueva normativa*. URL: https://eurocybcar.com/wp-content/uploads/2021/02/EUROCYBCAR_INFORME_normativa_ONU-UNECE-WP29.pdf (visitado 12-11-2022).

[3] Samy Kamar. "Defcon 23 (2015), Drive It Like You Hacked It". En: URL: https://samy.pl/defcon2015/.

[4] Rohde-Schwarz. *Tecnologías clave: sistemas de transmisión en automóviles*. URL: https://cdn.rohde-schwarz.com/magazine/pdfs_1/article/217/spanish_19/NEWS_217__01_RKE__es.pdf.

[5] secjuice - Matteo [0xless] Cosentino. *RKE: How To Hack A Car*. URL: https://www.secjuice.com/attacking-rke-how-to-hack-a-car-open/.

[6] A.I. Alrabady y S.M. Mahmud. "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs". En: *IEEE Transactions on Vehicular Technology* 54.1 (2005), págs. 41-50. DOI: 10.1109/TVT.2004.838829.

[7] R. Dawes. "HITB2022SIN Unlocking KeeLoq: A Reverse Engineering Story". En: 2022. URL: https://www.youtube.com/watch?v=Zr_NCoSH2cg.

[8] Grupo Premo. *Sistemas PKE*. URL: https://www.grupopremo.com/en/content/110-pke.

[9] Rushab Karani et al. "Implementation and design issues for using Bluetooth low energy in passive keyless entry systems". En: *2016 IEEE Annual India Conference (INDICON)*. 2016, págs. 1-6. DOI: 10.1109/INDICON.2016.7838978.

[10] *Tesla passive keyless netry system hacked*. URL: https://novelbits.io/tesla-passive-keyless-entry-system-hacked/.

[11] Wonsuk Choi, Minhye Seo y Dong Lee. "Sound-Proximity: 2-Factor Authentication against Relay Attack on Passive Keyless Entry and Start System". En: *Journal of Advanced Transportation* 2018 (ene. de 2018), págs. 1-13. DOI: 10.1155/2018/1935974.

[12] Ahmed Ghanem y Riham AlTawy. "Garage Door Openers: A Rolling Code Protocol Case Study". En: *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*. 2022, págs. 1-6. DOI: 10.1109/PST55820.2022.9851991.

[13] *HackRF One SDR*. URL: https://greatscottgadgets.com/hackrf/one/.

[14] *ANT500 telescopic antenna*. URL: https://greatscottgadgets.com/ant500/.

[15] *Yard Stick One. Hardware*. URL: https://greatscottgadgets.com/yardstickone/.

[16] *GNU Radio Companion software*. URL: https://www.gnuradio.org/.

[17] Wikipedia. *Codificación Manchester*. URL: https://es.wikipedia.org/wiki/Codificaci%C3%B3n_Manchester.

[18] *Datasheet Texas Instruments CC1110-CC1111 Wireless MCU*. URL: https://www.ti.com/lit/ds/symlink/cc1110-cc1111.pdf.

[19] *Librería rfcat para Python*. URL: https://github.com/atlas0fd00m/rfcat.

[20] *Datasheet 3DCoil isotropic SMD for Transponder - 20kHz - 3DC11LP-A-2000J*. URL: https://www.grupopremo.com/en/attachment?id_attachment=352.

Anexo A

Objetivos de Desarrollo Sostenible

En este capítulo se justifica la relación de este Trabajo Fin de Grado con los Objetivos de Desarrollo Sostenible (ODS) que fueron aprobados por la ONU en el año 2015, en la Agenda 2030 sobre el Desarrollo Sostenible.

Son 17 objetivos los que se marcaron, estos se pueden ver en la figura A.1. Se formularon con el fin de erradicar la pobreza, proteger el planeta y asegurar la prosperidad.

A priori, puede parecer que el concepto de sostenibilidad no tiene ninguna relación con la ciberseguridad, los vehículos y las nuevas tecnoogías. Pero sí hay un enlace. Por este motivo, este Trabajo de Fin de Grado se alinea con algunos de los 17 objetivos marcados.

En primer lugar, en la dimensión de la economía, el objetivo número 9 sobre Industria, innovación e infraestructura que tiene un rol primario expresa en la meta 11.2 "De aquí a 2030, proporcionar acceso a sistemas de transporte seguros, asequibles, accesibles y sostenibles para todos y mejorar la seguridad vial, en particular mediante la ampliación del transporte público, prestando especial atención a las necesidades de las personas en situación de vulnerabilidad, las mujeres, los niños, las personas con discapacidad y las personas de edad". Este objetivo se alinea claramente con los objetivos de este trabajo pues se trata de un proyecto de innovación cuyo objetivo es analizar el funcionamiento de tecnologías existentes en vehículos particulares para intentar mejorar sus características haciéndolos más seguros en el futuro. Además cabe destacar la reciente normativa sobre ciberseguridad aplicada a vehículos [2].

En segundo lugar, el objetivo número 11 sobre ciudades y comunidades sostenibles expresa en su meta número 9.1 "Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad, incluidas infraestructuras regionales y transfronterizas, para apoyar el desarrollo económico y el bienestar humano, haciendo especial hincapié en el acceso asequible y equitativo para todos" también guarda relación con la intención de este proyecto pues esta investigación hará posible mejorar los mecanismos de seguridad de vehículos futuros y con ello se reducirá el número de delitos relacionados con el robo de vehículos particulares, lo cual derivará en comunidades más sostenible.

Finalmente, una vez analizado en detalle las diferentes metas dispuestas en los Objetivos de Desarrollo Sostenible, se ve más claro que existe una relación justificada entre el proyecto y la sotenibilidad perseguida por la ONU.

Figura A.1: Objetivos de Desarrollo Sostenible

Anexo B

Librería rfcat

`rfcat` es una librería de Python que permite interactuar con el YARD Stick One y otros *dongles* basados en el chip C1111 de *Texas Instruments* [18] y permite desarrollar herramientas software de radiofrecuencia con mayor facilidad [19].

B.1. Requisitos

Para la instalación de `rfcat` es necesario un entorno linux como Ubuntu o Kali Linux. También hay una serie de paquetes que es necesario tener instalados para que la librería funcione correctamente:

- Python 2.7
- python usb
- libusb 1.x
- PySide2

B.2. Primeros pasos

Hay dos formas principales de trabajar con `rfcat`:

1. Trabajando en modo interactivo

2. Importando la librería en un script de Python

El modo interactivo resulta muy útil para realizar pruebas iniciales y para dar los primeros pasos con la librería, haciendo pruebas. Una vez comprendido el funcionamiento básico de la misma, es recomendable pasar a un script de Python.

B.2.1. Modo interactivo

Para iniciar el entorno interactivo se utiliza el comando `sudo rfcat -r`.

Una vez iniciado, se aparecerá en la consola de comandos un mensaje como el siguiente:

```
RfCat, the greatest thing since Frequency Hopping!'
Research Mode: enjoy the raw power of rflib
currently your environment has an object called "d" for dongle

this is how you interact with the rfcat dongle:
>>> d.ping()
>>> d.setFreq(433000000)
>>> d.setMdmModulation(MOD_ASK_OOK)
>>> d.makePktFLEN(250)
>>> d.RFxmit(b"HALLO")
>>> d.RFrecv()
>>> print(d.reprRadioConfig())
```

A continuación aparece un prompt donde se pueden introducir comandos.

Antes de nada, se deben configurar los parámetros necesarios para la recepción y transmisión de señales.

Algunos comandos básicos de configuración son:

- `d.setFreq(<Freq>)`: Establece la frecuencia de trabajo del dispositivo, expresada en hercios (Hz).

- `d.setMdmModulation(MOD_<modulation>)`: Establece el tipo de modulación que se va utilizar para TX (transmitir) o RX (recibir). Las modulaciones disponibles son:

  - 2FSK
  - GFSK
  - ASK/OOK
  - MSK
  - 2FSK/Manchester encoding
  - GFSK/Manchester encoding
  - 4FSK
  - ASK/OOK/Manchester encoding

    MSK está limitado a velocidades por encima de 26 kBaudios.

    GFSK, ASK, OOK no pueden superar 250 kBaudios.

    Cuando se utiliza MSK, la codificación Manchester debe permanecer desactivada.

- `d.setMdmPktLEN(<bytes>)`: Establece el tamaño de trama o paquete, se expresa en bytes.

- `d.setMdmDRate(<baudrate>)`: Define el *baudrate* o tasa de símbolos por segundo que se va utilizar para TX y RX. Expresado en baudios.

- `d.setEnableMdmManchester()`: Se debe activar si la señal que deseamos recibir utiliza codificación Manchester. En caso contrario deberá permanecer

en false.

Es importante destacar que cuando se estén modificando estos parámetros, el dispositivo debe permanecer en modo IDLE, este modo se activa haciendo uso del comando: `d.setModeIDLE()`

B.3. Modo librería

Para utilizar `rfcat` como librería para el desarrollo de scripts de Python, en necesario importar la librería `rflib` y crear un objeto que típicamente se llama `d` para utilizar los comandos descritos en la sección anterior. Y por último se puede utilizar las funciones `d.RFrecv` para recibir y `d.RFxmit` para transmitir.

A continuación, se muestra un ejemplo de script sencillo para la recepción de señales del vehículo A (código 1) y otro para la transmisión de códigos de apertura del vehículo B (código 2.

```
from rflib import *

d = RfCat(idx=0)
d.setMdmModulation(MOD_2FSK)    # Modulación 2FSK
d.setFreq(868300000)             # Frecuencia de trabajo
d.setPktPQT(29)              # Tamaño de paquete 29 bytes
d.setMdmSyncMode(1)          # Detectar como mínimo 4
                     # bytes de la palabra de sincronismo
d.setMdmDRate(2600)          # Baudrate 2.6k
d.setChannel(0)
#d.setPower(200)
d.lowball(1)                 # Deteccion de portadora
d.setEnableMdmManchester(1) # Codificación Manchester


print("Scanning...")
while True:

    try:
        y, t = d.RFrecv()
        yhex = hexlify(y).decode()

        print("(%5.3f) Received:  %s" % (t, yhex))

    except ChipconUsbTimeoutException:
        pass
    except KeyboardInterrupt:
        break

d.setModeIDLE()
```

Código 1: Script de ejemplo para la recepción de señales del vehiculo A con rfcat

```
from rflib import *

d = RfCat
d.setMdmModulation(MOD_ASK_OOK)  # Modulación ASK_OOK
d.setFreq(433900000)             # Frecuencia 433.9 MHz
d.setPktPQT(16)                  # Packet size 16 bytes
d.setMdmSyncMode(0)              # Sync word mode 0
d.setMdmDRate(2000)              # baudrate 2 kBd
d.setChannel(0)
d.setMaxPower()                  # Maxima potencia para mayor alcance
d.setEnableMdmManchester(0)

while True:

    try:
        data = bytes.fromhex(args.data)
        log.info(f'{INFO} Sending data: {data.hex()}')
        d.RFxmit(data)
        time.sleep(0.1)
    except ValueError:
        log_error(f'Bad hexadecimal data: {args.data}.')
    except ChipconUsbTimeoutException:
        usb_timeout()
    except KeyboardInterrupt:
        break

d.setModeIDLE()
```

Código 2: Script de ejemplo para la transmisión de señales del vehículo B con rfcat

Anexo C

Ficha técnica 3DCoil isotropic SMD for Transponder - 20kHz - 3DC11LP-A-2000J

También se puede encontrar accediendo al enlace en [20]

3DC11LP

SMD 3D Coil Low profile

13x11.6x3.20mm MAX (2.38mH – 7.2mH)

3-AXIS TRANSPONDER INDUCTOR (3DCOILS™)

APPLICATIONS

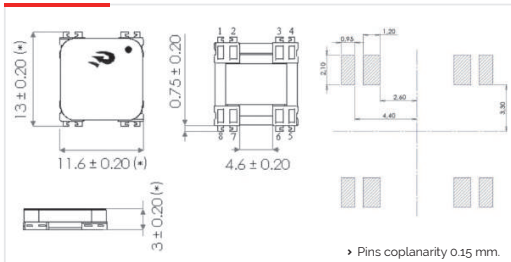
- Automotive Passive keyless entry systems.
- Automotive RTPMS with wake up functions.
- Industrial logistics and control.
- Access control.
- Tracking devices.

01 CHARACTERISTICS

- Offers 3 coils, oriented in the 3 space axes, assembled in a single component with full functionality.
- Suitable for automotive applications (Keyless Entry Systems, RTPMS), etc.
- Very good electrical performance in the smallest dimensions.
- High stability in temperature (-40°C to +85°C).
- High sensitivity values.
- The inductivity in each axis can be customized to achieve customer requirements.
- Designs at lower frequencies, 20 kHz or 40 kHz, show a very good electrical performance as well.

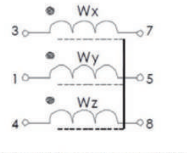
02 SPECIFICATIONS

DIMENSIONS AND RECOMMENDED PAD-LAYOUT (mm)



› Pins coplanarity 0.15 mm.

ELECTRICAL DIAGRAM



(2-3 and 6-7 are interconnected)

ELECTRICAL SPECIFICATIONS

P/N	L x,y,z (mH)	Qx,y,z Min	Freq (KHz)	Cres (pF)	SRFx,y (kHz) Min	SRFz (kHz) Min	DCRx,y (Ohm) Max	DCRx,y (Ohm) Max	Sensitivity x,y,z (mV/ App/m) Min	Length (mm)	Width (mm)	Height (mm)
3DC11LP-0238J	2.38	18	125	680	450	900	60,5	82,5	40	13	11,6	3,15
3DC11LP-0247J	2.47	17	125	656	450	900	68	82,5	40	13	11,6	3,15
3DC11LP-0345J	3.45	15	125	470	350	800	100	121	55	13	11,6	3,15
3DC11LP-0405J	4.05	15	125	400	300	600	100	138	60	13	11,6	3,15
3DC11LP-0477J	4.77	15	125	340	320	600	100	150	70	13	11,6	3,15
3DC11LP-0491J	4.91	18	125	330	300	600	100	160	70	13	11,6	3,15
3DC11LP-0720J	7.20	15	125	225	250	500	165	209	85	13	11,6	3,15
3DC11LP-A-2000J	20	5	20	3166	120	350	495	385	22	13	11,6	3,15

This chart is a reference guide for the most common required values at working frequency of 125 kHz. Any other inductance value at LF or tighter tolerances can be provided. Also can be supplied different inductance values in the different winding axis. Please contact our sales department for any inquiry.
L and Q factor measured at 125 kHz, 1 Vac.
Sensitivity measured with Helmholtz coils H=8.36 App/m @125 kHz. Contact us for measurement specification.
SRF: Self Resonant Frequency of the coil.