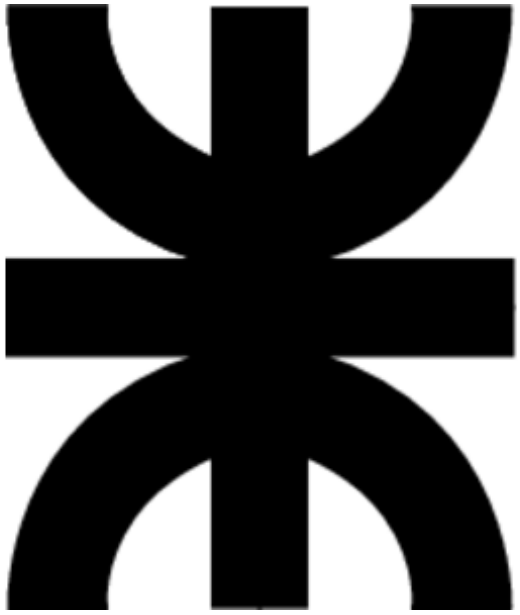

FACULTAD REGIONAL CÓRDOBA

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA

PROYECTO FINAL:

RED MULTINODAL PARA DETECTAR INHIBICIONES EN SISTEMAS DE SEGURIDAD VEHICULAR

Coronel Martín, Fantin Stéfano, Giletta Julian

Docentes evaluadores:
Candiani, Carlos
Rabinovich, Daniel
Galleguillo, Juan

Agradecemos profundamente a nuestra familia
que siempre nos apoyó en este largo camino
y a la Universidad Tecnológica Nacional,
particularmente a la carrera de ingeniería electrónica, la cual siempre se caracterizó por la buena organización y la búsqueda del bienestar estudiantil.

Resumen

En este documento se plasma el proceso de investigación y desarrollo de un sistema multinodal pensado para detectar inhibiciones en los sistemas de seguridad vehicular que funcionen en la frecuencia de 433,92MHz.
El dispositivo planteado cuenta con tres unidades de recepción, las cuales denominamos nodos, y una central de procesamiento encargada de comunicarse y gestionar la información por estos recolectada.
Para la comunicación entre los nodos y la central se utiliza el protocolo RS485, y para comunicar la central con un servidor web, teniendo así los datos a disposición remotamente, se hace uso de un módulo GSM.

Índice general

Índice de figuras

Índice de cuadros

Capítulo 1

Introducción

Hoy en día en muchos paises, y particularmente en la Argentina, se presenta una recurrente modalida de delincuencia que trata de inhibir los sistemas de seguridad vehicular, no permitiendo que estos se cierren y pudiendo tener completo acceso a su interior. Es una metodología muy usada debido a que no se hace uso de la fuerza bruta para ingresar al vehículo y apela a la distracción del usuario.
Siendo conscientes de esta problemática nos hemos empeñado en desarrollar un sistema de detección de los dispositivos utilizados con este fin. Como se verá más adelante se ha hecho un relevamiento de los dispositivos incautados por la policía a través de notas periodísticas y con vínculos internos a departamentos policiales que pusieron a disposición la información presente sobre estos.
Los inhibidores pueden operar corrompiendo la trama de datos emitida por el llavero, no dejando así que el receptor del vehículo pueda identificar el intento de comunicación y también lo pueden hacer saturando el receptor, cosa que de igual manera este no puede identificar la comunicación intentada. Creemos importante que el dispositivo a diseñar abarque estas dos posibilidades.
Otra característica importante a la hora de encarar el proyecto es determinar la frecuencia de operación. Los controles remotos poseen transmisores de radio de corto alcance que operan en dos bandas posibles: 433,92 MHz para vehículos de origen europeo y asiático y 315 MHz para vehículos de origen norteamericano. En la Argentina la mayor cantidad de sistemas de seguridad operan en 433,92 MHz por lo que nos pareció adecuado diseñar el detector para esta frecuencia.

Una vez definidos los requerimientos básicos del desarrollo es importante establecer el lugar en el que creemos adecuado que opere. Es así que surge la idea de tener al menos tres nodos receptores capaces de identificar si hay o no un inhibidor en las inmediaciones de este y que la información que recolecte sea enviada a una unidad de procesamiento, que denominamos "central", la cual se encargaría de comunicarse con los nodos, recopilar la información y subirla a una base de datos, permitiendo la visualización remota de lo que está sucediendo en tiempo real y, de ser posible, triangular la posición estimada del dispositivo inhibidor dentro del arreglo de receptores.
Esto sería emplazado en un estacionamiento utilizando una estrategia de disposición que se analizará más adelante

1.1. Marco teórico

Es importante realizar un estudio profundo sobre el tema que vamos a abordar, ya que es necesario definir un método novedoso que satisfaga la necesidad de distinguir interferencias de señales legítimas generadas por un control remoto.

1.1.1. Codificación en sistemas de seguridad vehicular

Desde los inicios de los sistemas remotos de apertura y control vehicular hasta ahora se ha transitado un largo camino. El primer sistema de identificación por radiofrecuencia fue ingresado en el mercado por Renaul en el modelo Fuego en el año 1995. Todo este tiempo desde su puesta en uso hasta la fecha ha servido para definir y universalizar las metodologías usadas para comunicarse, intentando dar una mejora en cuanto a la seguridad y efectividad del sistema.

Sistemas de código fijo

Esta es la forma más difundida de codificación para los controles remotos vehiculares en nuestro país. Se trata de un código de comunicación fijo, que precisa estar preestablecido en el circuito integrado del dispositivo, el cual se mantiene constante para la acción a realizar. De esto podemos notar que para los controles remotos comunes que poseen opción de cierre y apertura

del automóvil se tienen solo dos códigos fijos que realizan cada una de estas acciones y que, eventualmente, podrían ser copiados y replicados para generar la acción codificada.

Sistemas de código variable

Esta metodología no está muy difundida en nuestra región. Se trata de un sistema de seguridad que no repite el mismo patrón para ejecutar la acción de cierre o apertura del vehículo para evitar que se pueda leer y replicar el código. Usualmente se hace uso de un generador de números pseudoaleatorios que se encuentra en el emisor y receptor, un contador de pulsaciones en el emisor y un contador de recepciones en el vehículo. Cuando el control remoto envía la señal para realizar una acción en el vehículo este manda su contador, el cual será comparado con el interno del receptor y, de estar dentro de la ventana de aceptación definida en el sistema de seguridad, el automóvil autentica el mensaje recibido y actualiza el contador interno, ya que este puede diferir al de la llave. Hay diversos tipos de encriptación de la comunicación; aquí solo mencionaremos los más difundidos: Hitag 1, Hitag 2, Hitag AES, DST-40, Keeloq

Sistemas por desafío

El sistema por desafío es actualmente el más utilizado en autos de alta gama. En este caso el control remoto intenta comunicarse y el vehículo envía una pregunta desafío que tiene que ser respondida correctamente para validar la comunicación.
En esta variante por lo que fpácilmente se puede observar es necesario que el control remoto y el vehículo tengan la capacidad de emitir y recibire datos, generando una comunicación bidireccional. Hay muchas variantes de desafío requerido por el vehículo, pero la más utilizada es la de validación de contraseña, donde el desafío pedido es pedir la contraseña y esta será o no validada. Esto en definitiva no impide que sea replicado el patrón de comienzo de comunicación y la autenticación, por lo que hay modalidades más avanzadas como tener una tabla de códigos pseudoaleatorios definida en ambos dispositivos y asociada a un identificador, de modo que el vehículo requiera el código por medio de este no dando lugar a que un escucha externo pueda saber a qué valor está asociado.

1.1.2. Estructura de transmisión

Tener noción previa de lo que esperamos recibir cuando hacemos un análisis de una señal es de gran importancia, por lo que en esta sección analizaremos la estructura de transmisión de un control remoto de autos.
Como antes fue mencionado no hay solo una frecuencia de operación, pero sí hay una que es ampliamente difundida en nuestro país y en esa nos centraremos (433,92 MHz), la modulación utilizada en la mayor cantidad de estos dispositivos es ASK, por su fácil implementación. Con esta información ya seríamos capaces de demodular la señal y analizar la estructura.
Para la demodulación de la señal hemos utilizado un SDR (Software Defined Radio) como el que se puede observar en la figura 1.1, el cual fue facilitado por el centro de investigación G.In.T.E.A (Grupo de Investigación y Transferencia en Electrónica Avanzada) de la Universidad Tecnológica Nacional, facultad regional Córdoba.

Figura 1.1: Software Defined Radio utilizado para tomar las primeras mediciones

En la figura 1.2 podemos observar las primeras mediciones tomadas. Aquí podemos distinguir la estrategia de transmisión que se utiliza. En un comienzo la señal posee un preámbulo, el cual es utilizado por el receptor para sincronizar el reloj del receptor para decodificar correctamente los paquetes del transmisor. Después del preámbulo hay una palabra de sincronización que se utiliza para evitar choques con otros dispositivos que operan en esa banda y por último se encuentra la señal de código real.

Al presionar el botón del control remoto el preámbulo es enviado una única vez y luego se envía la palabra de sincronización y el comando de acción repetidamente hasta que se deje de accionar.

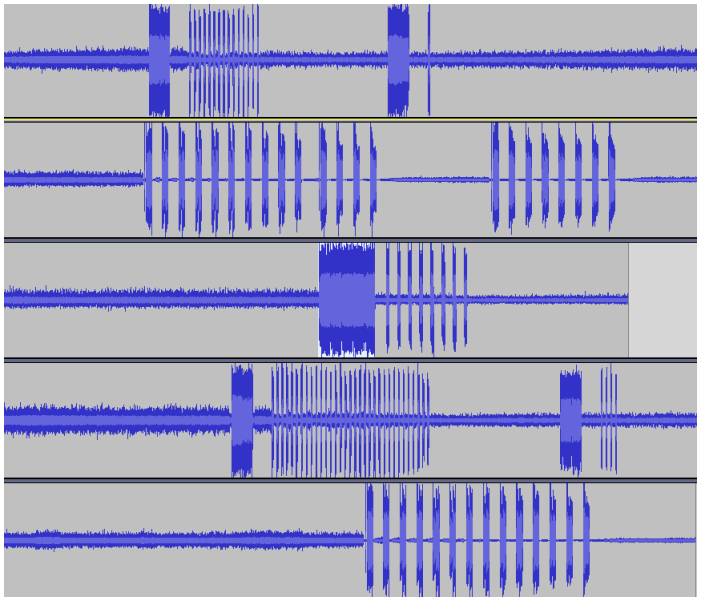

Figura 1.2: Demodulación ASK de señales de controles remotos en 433,92 MHz

1.1.3. Tipos de inhibiciones

Un inhibidor, o en inglés jammer, es un dispositivo desarrollado con el objetivo de deteriorar la comunicación en un enlace de radiofrecuencia. Este objetivo puede ser logrado mediante dos estrategias:

- Inhibición por corrupción de datos
- Inhibición por saturación de etapa receptora

Inhibición por corrupción de datos

El ataque más evidente que se presenta para inhibir una comunicación es el de inyectar en el canal que se desea perjudicar una señal con datos aleatorios que perjudique la relación señal ruido (SNR) y dificulte la recepción

para el sistema.
En el caso particular de los vehículos, los receptores de radiofrecuencia que se utilizan y sobre los que basamos nuestro análisis son de 433,92 MHz con un filtro de ancho de banda de entrada de 300 KHz -como se puede observar en [1] AGREGAR REF A datasheet de MAX147-.
El ancho de banda de recepción da lugar a sumar ruido en el canal, alterando así los datos recibidos por el demodulador. Una figura ilustrativa se puede observa en la imagen 1.3 de referencia a carhackerhandbook [2].

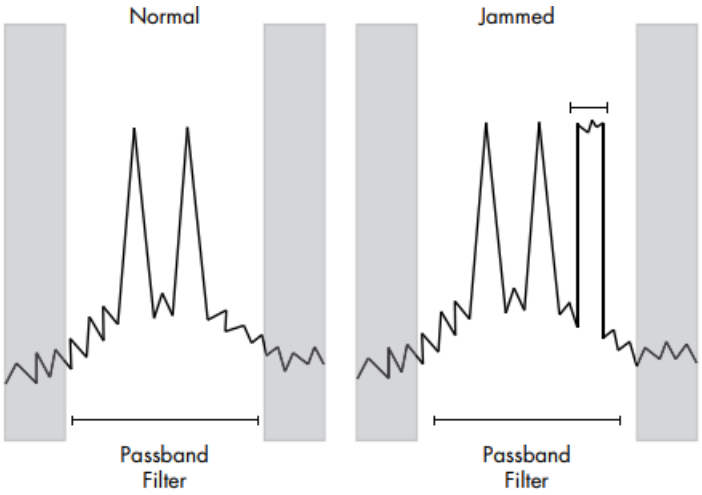

Figura 1.3: Presencia de inhibidor en ancho de banda de recepción

Existen diversas alternativas para efectivizar este tipo de interferencias. En la figura 1.3 se observa que se ha inyectado una interferencia de ancho de banda angosto, pero también podría sumarse un tono, multitonos o sumar una señal de gran ancho de banda que tape completamente el canal.
Las alternativas antes mencionadas hacen referencia a inhibidores no inteligentes, los cuales están metiendo ruido constantemente. Hay otras alternativas de inhibiciones que de manera continua están escuchando el canal y cuando detectan una señal que desean interferir comienzan a emitir el ruido. Estos casos serán detallados más adelante.

Inhibición por saturación de etapa receptora

Los receptores de radiofrecuencia usualmente están diseñados asumiendo que se recibirá una pequeña señal de entrada, por lo que la primer etapa presente es un amplificador de bajo ruido. Este es clave para que el ruido del mezclador no afecte la relación señal ruido de las etapas siguientes. Entre las especificaciones importantes de dichos amplificadores de RF se incluyen la figura de ruido, la ganancia y la intercepción de intermodulación de tercer orden.

[6]-[7] La influencia de grandes señales de interferencia se manifiesta de varias formas. Una de estas es en la intermodulación de tercer orden en la que dos señales, una pequeña (de interés) y la interferente (de gran amplitud), se superponen. La interferente podría saturar el receptor de modo que la señal de interés presente una pequeña ganancia. Este efecto es causado por la no linealidad de tercer orden del sistema y la relación entrada salida está regida por 1.1.

$$y(t) \approx a_1 x(t) + a_2 x^2(t) + a_3 x^3(t) \tag{1.1}$$

Donde y es la salida del sistema y a_1, a_2, a_3 son coeficientes. Ahora supongamos que la entrada, como es de esperar con lo antes descripto, resulta:

$$x(t) = V_1 cos(\omega_1 t) + V_2 cos(\omega_2 t) \tag{1.2}$$

V_1 representando a la señal de interés y V_2 a la interferente.
Reemplazando en la ecuación 1.2 en 1.1 y asumiendo que la interferencia es mucho más grande que la señal, la salida del sistema en la frecuencia de interés ω_1 resulta ser 1.3.

$$y(t) \approx \left(a_1 x(t) + \frac{3}{2} a_3 V_2^2 \right) V_1 cos(\omega_1 t) \tag{1.3}$$

Para que el sistema comprima la ganancia, como es evidente que sucede, el producto $a_1 a_3 < 0$. De aquí se puede observar entonces que la salida del sistema en la frecuencia deseada es función de V_2^2, que la ganancia decae saturando el sistema y por ende se decrementa la SNR. Esto es fácilmente observable en la figura 1.4.

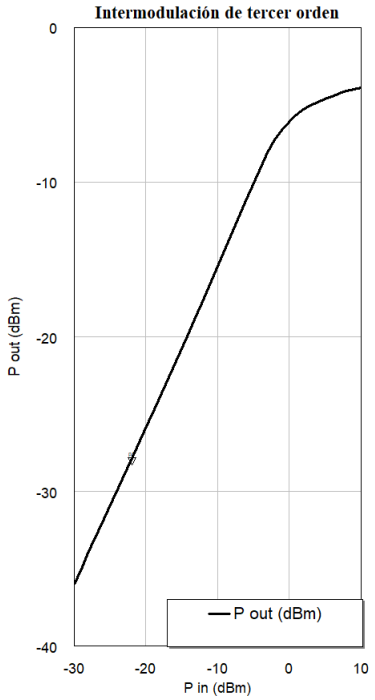

Figura 1.4: Compresión de la ganancia por no linealidad de tercer orden

1.1.4. Estrategias de inhibición

Antes hemos presentado los principios de inhibición que se pueden utilizar, en este apartado se tratará de una manera generalizada las diversas estrategias existentes para inhibir sistemas de comunicación. Cada una de estas estrategias tienen ventajas y desventajas, por lo que es necesario hacer un análisis del ámbito de aplicación para elegir la más adecuada.

Inhibición por ruido de banda ancha

La característica principal de este tipo de estrategia es que introduce energía dentro de todo el ancho del espectro donde opera la comunicación. Es aplicable a cualquier tipo de señal y es ideal para inhibir comunicaciones que tienen destinada una gran parte del espectro de frecuencias.
Este método tiene una fuerte desventaja y es que la potencia de interferencia aportada en el canal deseado tiene una muy baja densidad debido a es

aplicada a un gran ancho de banda.

Inhibición por ruido de banda parcial

Este método opera inyectando ruido en bandas específicas del espectro, de modo que se efectúa la inhibición en zonas de interés. Estas zonas pueden ser continuas o discontinuas, por lo que se destina más inteligentemente la potencia consumida. El ejemplo más trivial aplicado a nuestro campo sería el de un inhibidor que funcione en 433,92 y en 315 MHz, siendo aplicable a todos los canales de comunicación de controles remotos.

Inhibición por ruido de banda angosta

Esta caso es el más utilizado en el campo de inhibición sobre el que nos centramos ya que permite puntualizar la potencia en una pequeña banda aumentando la densidad de potencia espectral. Para su aplicación es necesario conocer precisamente el canal a atacar debido a que las comunicaciones innalámbricas de banda angosta poseen un angosto filtrado.

Inhibición por tono

Se utiliza una señal constante que se modula con la portadora resultando una señal de muy angosto ancho de banda. En sistemas de comunicación avanzados posee una alta eficiencia de interferencia ya que perjudica la recuperación de la sintonización a causa de que el receptor detecta la señal como una segunda portadora y de que más potencia por Hertz (densidad de potencia espectral) gracias a que está más concentrado en el canal, como profundamente se analiza en [8].

Inhibición por pulsos

En esta estrategia nos enfocamos en el tiempo que se genera la interferencia. Se hace uso de uno de los métodos anteriores de inhibición y se desata la misma de manera inteligente. De aquí surge el concepto de aplicar la estrategia a casos específicos, permitiendo, por ejemplo: romper tramas específicas de datos conocidas cuando se detecta un CLT/RTS, interferir el dato de direccionamiento MAC o romper exclusivamente la trama de datos.

Inhibición por barrido y seguimiento

Esta es una aplicación del ruido de banda parcial. Se realiza una variación rápida del posicionamiento espectral de la interferencia para inhibir un gran ancho de banda teniendo un mejor aprovechamiento de la potencia disponible.
De esta alternativa se desprende la capacidad de seguimiento de la señal inhibidora, permitiendo contrarestar estrategias de comunicación que hacen uso de saltos de canales para ser efectivas.

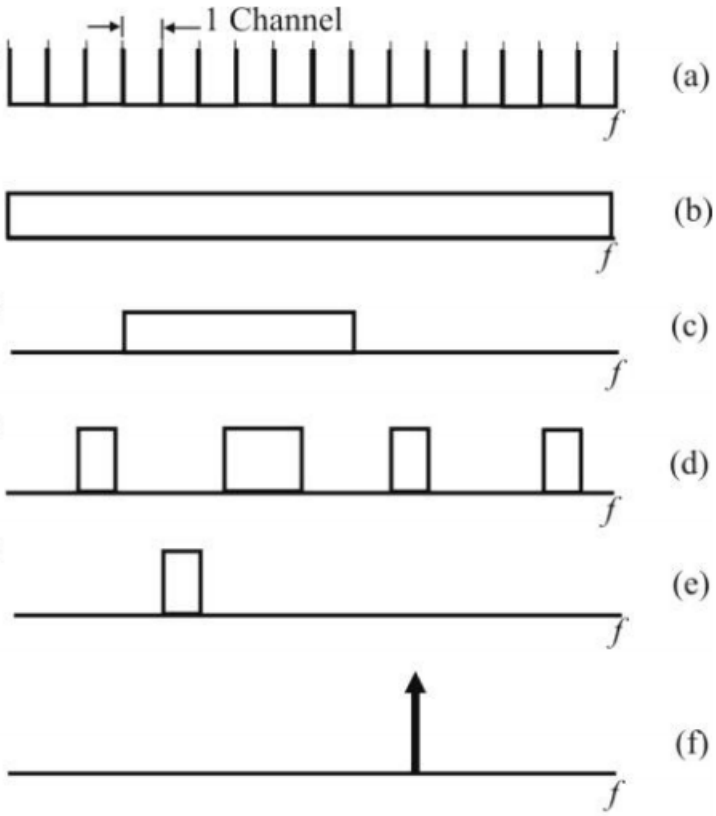

Figura 1.5: Donde a) es el canal a inhibir, b) inhibición por ruido de banda ancha, c) inhibición por ruido de banda parcial continuo, d) inhibición por ruido de banda parcial discontinuo, e) inhibición por ruido de banda angosta, f) inhibición por tono

1.2. Objetivos de la investigación

En base a la información recolectada establecemos los capacidad de detectar inhibicion de potencia o corrupcion Una forma de atacar la señal de un llavero es atascándola pasando datos basura dentro de la banda de paso del receptor RFID, el área en la que el receptor está escuchando una señal válida (pagina 217 imagen)