

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 GPRS.

Índice general

Resumen	II
1. Introducción	1
1.1. Marco teórico	2
1.1.1. Codificación en sistemas de seguridad vehicular	2
1.1.2. Estructura de transmisión	3
1.1.3. Tipos de inhibiciones	5
1.1.4. Estrategias de inhibición	8
1.1.5. Detección de inhibiciones	12
2. Características generales del diseño	16
2.1. Objetivos globales del sistema	16
2.2. Esquema de funcionamiento	17
2.3. Subsistemas que lo componen	18
3. Nodos de recepción	19
3.1. Descripción general	19
3.2. Prototipo	19
3.3. Diseño final	21
3.3.1. Software	21
4. Desarrollo de servidor web	24
4.1. Objetivos	24
4.2. Página web	25
4.2.1. Pestañas	27
4.3. Base de datos	31
4.3.1. Carga de datos	31



5. Conclusiones y trabajo futuro	32
5.1. Conclusiones	32
5.2. Trabajo futuro	33

Índice de figuras

1.1. Software Defined Radio utilizado para tomar las primeras mediciones	4
1.2. Demodulación ASK de señales de controles remotos en 433,92 MHz	5
1.3. Espectro de señal random bits modulada ASK en 433,92 MHz	6
1.4. Presencia de inhibidor en ancho de banda de recepción	7
1.5. Compresión de la ganancia	9
1.6. 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	11
1.7. Diagrama en bloques de sistema de comunicación ASK inhibido	12
1.8. Bit Error Rate para comunicación ASK inhibida.	13
1.9. Curva de ganancia de MAX1470	14
2.1. Diagrama en bloques sobre el funcionamiento del sistema global	18
3.1. Asignación de pines para comunicación	20
3.2. Estrategia de detección por corrupción de datos	23
3.3. Estrategia de detección por saturación de etapa receptora . . .	23
4.1. Página de inicio	27
4.2. Presentación de grupo de trabajo	28
4.3. Gráficos de estadísticas	28
4.4. Pestaña de triangulación	30
4.5. Formulario de contacto	30

Capítulo 1

Introducción

Hoy en día en muchos países, y particularmente en la Argentina, se presenta una recurrente modalidad 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. También lo pueden hacer saturando el receptor. 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 señales legítimas generadas por un control remoto de interferencias.

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 Renault 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 se puede observar que es necesario que el control remoto y el vehículo tengan la capacidad de emitir y recibir datos, generando una comunicación bidireccional. Hay diversas opciones de desafíos de requerimiento realizados por el vehículo, pero la más utilizada es la de validación de contraseña, donde el desafío 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 analiza-



remos 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 distinguimos 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. El espectro de la señal transmitida se puede observar en la figura 1.3, la cual es una simulación en el software AWR de una transmisión de datos random modulados ASK.

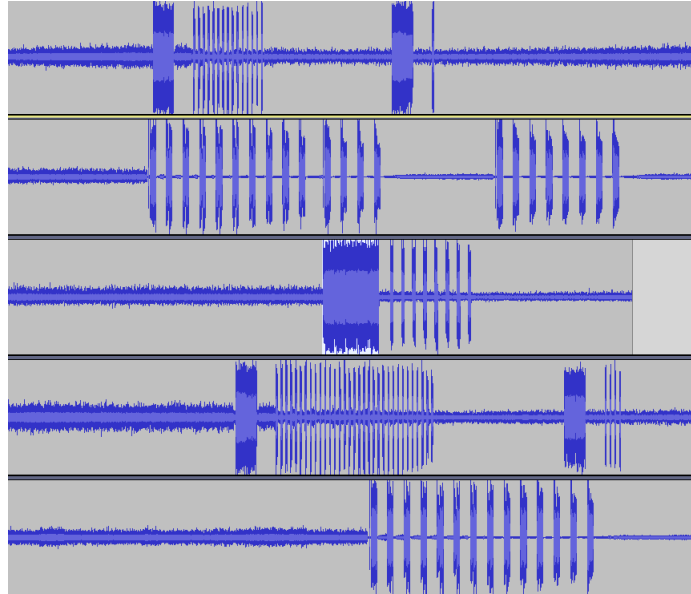


Figura 1.2: Demodulación ASK de señales de controles remotos en 433,92 MHz

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. Esto 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 analiza en [1].

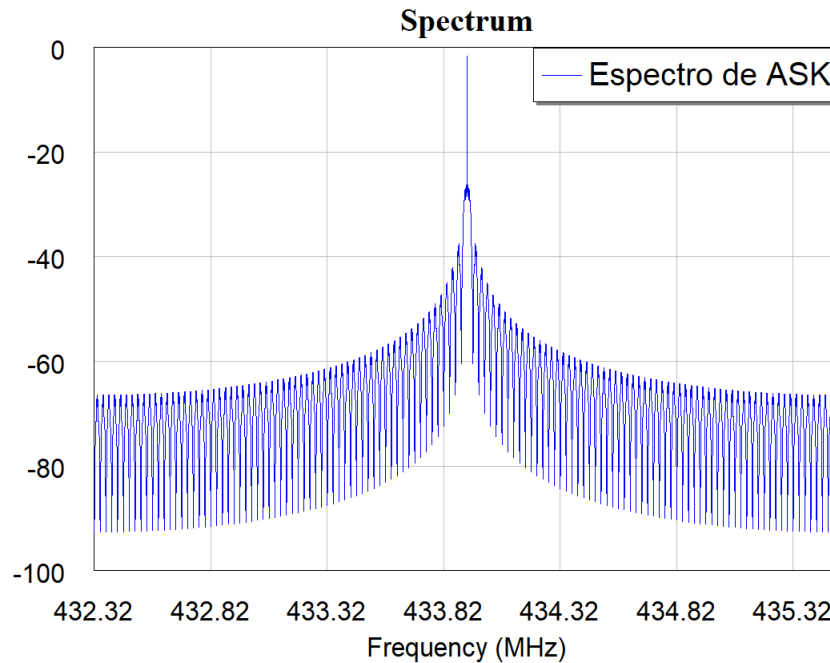


Figura 1.3: Espectro de señal random bits modulada ASK en 433,92 MHz

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 observar en la imagen 1.4 de [2].

Existen diversas alternativas para efectivizar este tipo de interferencias. En la figura 1.4 se observa que se ha inyectado una interferencia de ancho de banda angosto, pero también podría sumarse un tono, multitonos o sumarse 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.

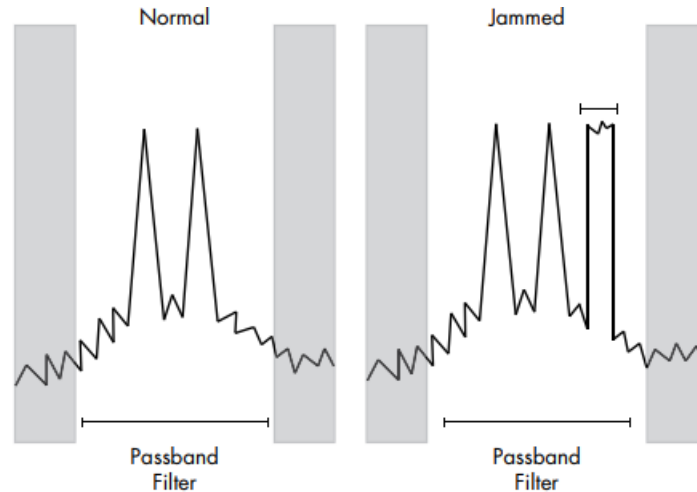


Figura 1.4: Presencia de inhibidor en ancho de banda de recepción

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.

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 como hace referencia [6] y [7]. Este efecto es causado por la no linealidad de tercer orden del sistema.

La saturación de un sistema suele tener un comportamiento de compresión de la ganancia, decrementando la misma a medida de que la entrada aumenta. Este efecto puede ser cualificado como el punto de 1 dB de compresión el cual está definido como el punto en el que la amplitud de la señal de entrada genera que la ganancia caiga 1 dB. Esto antes mencionado está claramente ilustrado en la figura 1.1.



$$y(t) \approx a_1x(t) + a_2x^2(t) + a_3x^3(t) \quad (1.1)$$

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:

$$x(t) = V_1\cos(\omega_1t) + V_2\cos(\omega_2t) \quad (1.2)$$

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.

$$y(t) \approx \left(a_1x(t) + \frac{3}{2}a_3V_2^2 \right) V_1\cos(\omega_1t) \quad (1.3)$$

Para que el sistema comprima la ganancia, como es evidente que sucede, el producto $a_1a_3 < 0$. 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 1.5.

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 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.

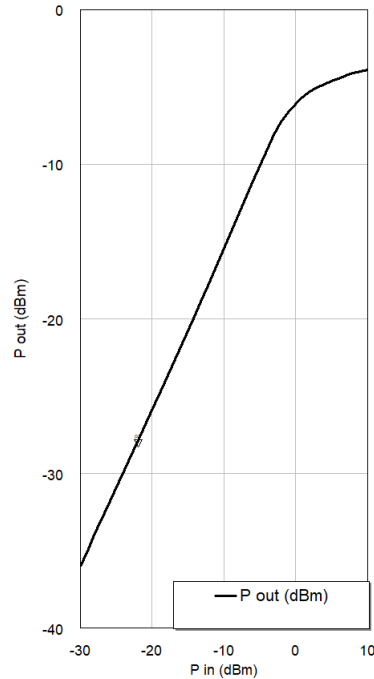


Figura 1.5: Compresión de la ganancia

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 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

Este 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 inalámbricas 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 contrarrestar estrategias de comunicación que hacen uso de saltos de canales para ser efectivas.

Simulación de inhibición por ruido de banda parcial

En este apartado se ha elegido la metodología de inyección de ruido de banda parcial para ser simulado y mostrar como decae la calidad de comunicación y, por ende, la capacidad de recepción de la información. La simulación fue realizada con el software AWR de Cadence.

El diagrama en bloques se puede observar en la figura 1.7, este cuenta de 4 secciones principales:

- Inhibidor de potencia variable: este bloque inyecta ruido blanco al sistema en la frecuencia definida como portadora, que en nuestro caso es

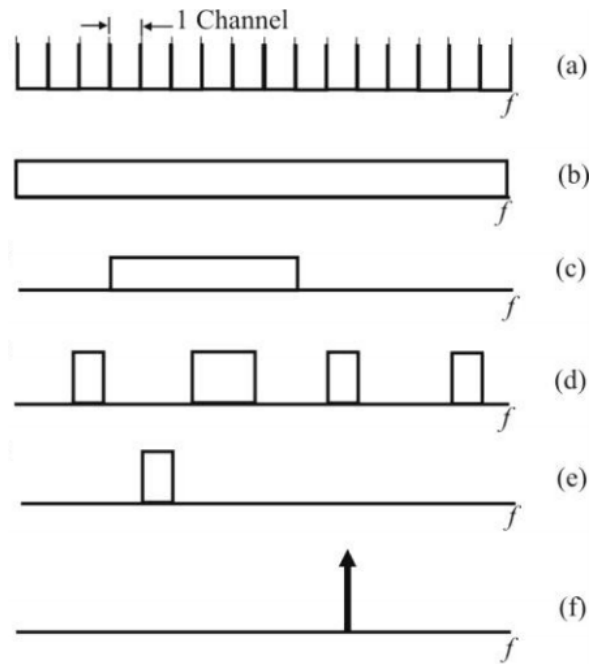


Figura 1.6: Donde a) es el canal a inhibir, b) inhibición por ruido de banda ancha, c) inhibición por ruido de banda parcial continuo, d) inhibición por ruido de banda parcial discontinuo, e) inhibición por ruido de banda angosta, f) inhibición por tono

433,92 MHz. La potencia de ruido va a variar entre 0 y -30 dBW, lo que sería igual a decir entre -30 y -60 dBm.

- Emisor de señal: el emisor de señal es un modulador de ASK que modula una generación aleatoria de bits a 2500 baudios con la portadora.
- Medio de enlace: en este caso está representado con un combinador de señal RF, el cual va a servir para sumar la potencia de las dos señales anteriores.
- Demodulador: en esta instancia se produce la demodulación de la señal ASK más el ruido blanco agregado. Al final posee un bloque que se encarga de controlar el BER (Bit Error Rate), chequeando cuántos datos de los enviados efectivamente fueron recibidos.

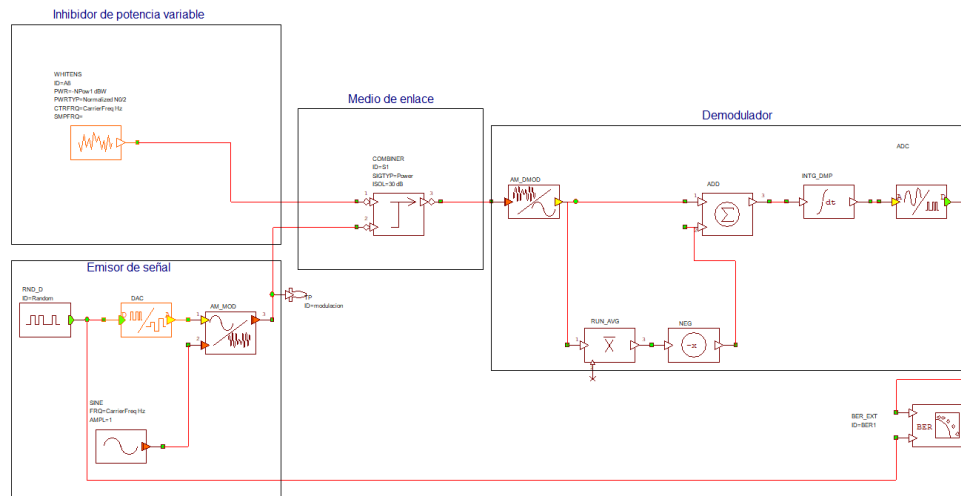


Figura 1.7: Diagrama en bloques de sistema de comunicación ASK inhibido

Como antes se menciona, y como se puede observar en la figura 1.8, el error de recepción alcanza su valor máximo cuando el ruido inyectado es de 0 dBW (-30 dBm). En la figura se puede leer un valor de $BER = 0.4866$, el cual es lógico debido a que la modulación ASK solo posee dos símbolos, por lo que la probabilidad de que coincida el dato generado por el ruido y el esperado es del 50 %. Por otro lado el valor mínimo de error en la simulación propuesta sucede cuando la potencia del inhibidor es de -30 dBW (-60 dBm) teniendo un error de cuatro bits por cada diez mil recibidos.

1.1.5. Detección de inhibiciones

En esta sección trataremos los métodos que pueden utilizarse para detectar interferencias en enlaces de radiofrecuencia. Es importante que sea robusta la detección, en principal que el funcionamiento del sistema que se pretende asegurar no pueda desatar una falsa alarma. En el caso puntual de aplicación de este proyecto, el sistema debería poder identificar una inhibición y no identificar como tal a las señales de controles remotos que van a estar funcionando en el área circundante. Hay algunas características las cuales son naturales pensar como sensibles de analizar para detectar inhibiciones, y estas son:

- Potencia de la señal recibida

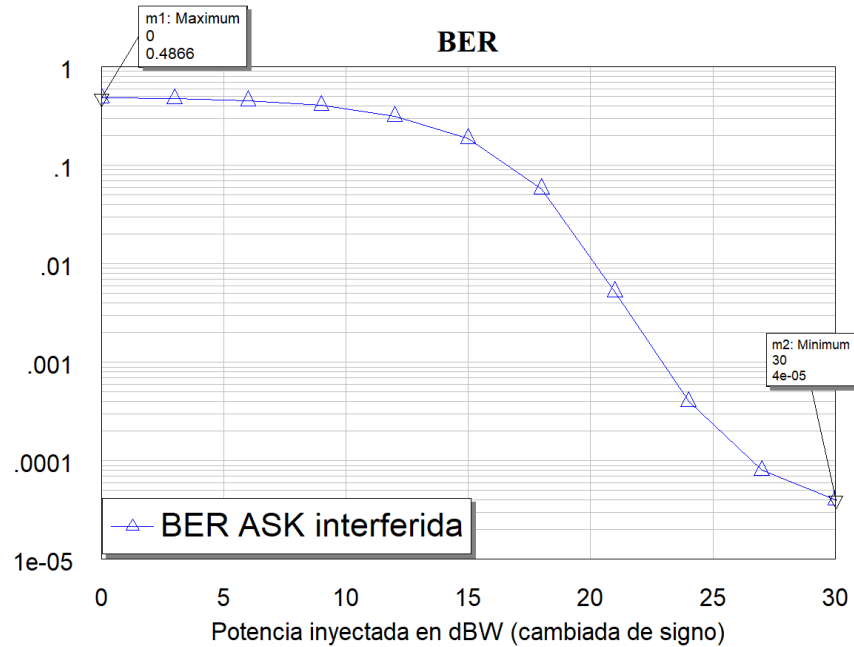


Figura 1.8: Bit Error Rate para comunicación ASK inhibida.

- Sensado temporal de portadora
- Ocupación del canal

Potencia de la señal recibida

Como antes se ha definido, el receptor sufre compresión de ganancia en su primera etapa amplificadora cuando la potencia recibida es alta comparado a la potencia de señal que se espera recibir y para el que fue diseñado. Es por esto que resulta natural analizar los niveles de potencia recibidos, estableciendo un valor a partir del cual se señale como alarmante para la correcta recepción de la información. En el caso particular de los dispositivos de control remoto en los sistemas de seguridad vehicular resulta más sencillo el análisis debido a que los dispositivos emisores que se utilizan son de baja potencia comparado a la necesaria para saturar un receptor típico.

En [7] se realiza el análisis del receptor MAX1470 [1], muy difundido en sistemas de control remoto tanto en el ámbito automotriz como también en sistemas de portones de apertura inalámbrica, sistemas de seguridad, sensores



inalámbricos y mucho más. Este integrado es un receptor de ASK superheterodíneo de bajo costo que posee un mezclador de rechazo de imagen que mezcla la señal a una frecuencia intermedia de 10,7 MHz. En la figura 1.9 se puede observar que la ganancia del sistema de recepción se aplana aproximadamente con una entrada de -35 dBm.

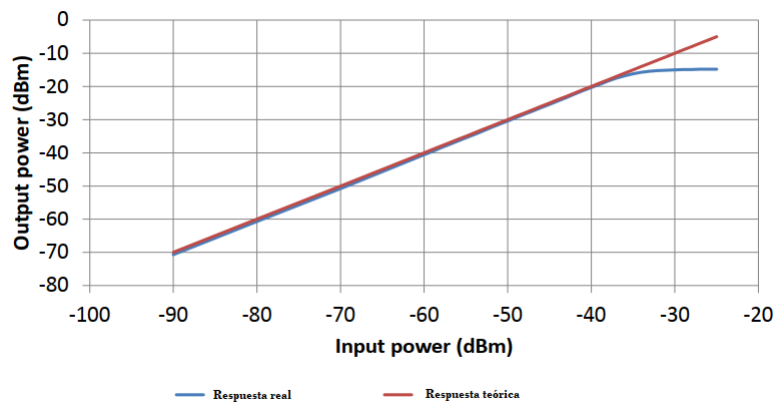


Figura 1.9: Curva de ganancia de MAX1470

Sensado temporal de portadora

Esta es una estrategia muy utilizada en sistemas de comunicación en que se realiza un envío efectivo de paquetes cuando se detecta que el canal de transmisión está desocupado. Esta característica hace sensible al sistema de ser engañado dejando presente una señal portadora de información que engañe a los dispositivos emisores de la red.

En nuestro caso no nos detendremos a hacer un análisis profundo de esta metodología ya que es ajena a nuestro potencial mecanismo de detección debido a que, como se menciona en 3.1.2, el control remoto emite señal cuando es accionado un botón que este posee, haciéndolo de manera continua hasta que deje de ser apretado. Es fácil ver que esta característica de la comunicación hace inútil aplicar esta estrategia de detección.

Ocupación del canal

El sistema de comunicación que nos basamos para desarrollar este trabajo tiene la particularidad de que la comunicación unilateral que sucede



entre los dispositivos de emisión (controles remotos) y recepción (vehículos) tienen una muy baja tasa de ocupación de canal. Esto se debe a la trama de datos empleada. La misma, como antes fue explicado, posee un período de sincronización que es una rápida variación de estados, para que el receptor pueda engancharse en fase a la recepción, y luego envío de paquetes de datos separados por espacios vacíos de información. Esta característica nos da una relación de bits en alto recibidos respecto a los medidos de un valor porcentual muy bajo. Es por esto que esta medición en el canal, usandola estratégicamente, nos puede dar mucha información de lo que está sucediendo.

Capítulo 2

Características generales del diseño

2.1. Objetivos globales del sistema

En base a la información recolectada establecemos los requerimientos base del que se parte para el diseño del producto final. Creemos adecuado realizar la separación de requerimientos en primarios y secundarios, ya que el sistema a desarrollar está enmarcado en el proyecto final de la carrera de grado de ingeniería electrónica donde, en conjunto con la cátedra, se intenta que los proyectos puedan culminarse en un plazo de tiempo lógico para la obtención del título, dando la posibilidad de seguir explayándose en el mismo a posterior.

De este modo, como objetivos primarios se establecen:

- Identificar la presencia de señales con una potencia suficiente para inhibir la comunicación: como en el marco teórico se ha estudiado en profundidad, la etapa amplificadora receptora sufre una compresión de la ganancia cuando en su entrada hay presente una señal de alto nivel de potencia. Es por esto que se establece como requerimiento del sistema poder identificar una señal que cumpla con estas características.
- Medir la ocupación del canal: Ha quedado claro que la trama de comunicación de las llaves remotas con los receptores de los automóviles poseen características de espaciado entre paquetes de datos transmitidos, es por esto que el sensado de la ocupación del canal se vuelve una



medida crucial para determinar si hay o no presencia de interferencias.

- Activar alarmas sonoras y visuales en caso de estar en presencia de una inhibición: el sistema debe tener la capacidad de determinar si hay presente una inhibición en su área de operación y, de ser así, debe disponer de métodos para dar alerta local de lo que está sucediendo.
- Disponer de comunicación a sistemas externos complementarios: un requisito del sistema es que posea la capacidad de enviar la información recolectada a un lugar remoto. Se prefiere la utilización de una metodología de comunicación inalámbrica y ampliamente distribuida.
- Cargar los datos en una base de datos: es importante que la información de las inhibiciones detectadas sea subida a una base de datos que permita visualizar de manera remota y en tiempo real lo que está sucediendo con los sistemas de seguridad activos, brindando la posibilidad de generar estadísticas y observar qué tipos de inhibidores están operando en la zona.
- Orientar el diseño del proyecto a la optimización de costos y recursos: es muy importante para el curso del trabajo que el diseño se realice haciendo uso racional de los recursos disponibles, apuntando a la posibilidad de producir muchas unidades del sistema de seguridad y obtener ganancias.

Como objetivo secundario se define:

- Estimar la procedencia de la interferencia: el único objetivo secundario del sistema es que tenga la capacidad, mediante el método más conveniente, de determinar la posición estimada de la fuente de interferencia activa. Esto está planteado de esta manera debido a que se desconoce la factibilidad de su realización en el marco del proyecto de fin de grado de ingeniería electrónica.

2.2. Esquema de funcionamiento

En la figura 2.1 se puede observar el sistema planteado para solucionar el desafío de detectar inhibiciones en los sistemas de seguridad vehicular. El mismo contará con nodos detectores que operarán en 433,92 MHz, un canal



de comunicación hacia la central, haciendo uso de un protocolo que más adelante se detallará y una central de operación donde se decidirá si hay o no inhibición en su área de operación desatando las alarmas pertinentes y subiendo la información al servidor.

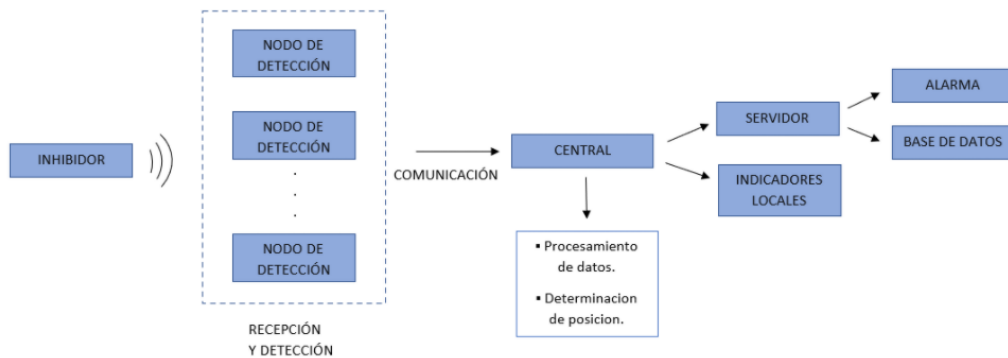


Figura 2.1: Diagrama en bloques sobre el funcionamiento del sistema global

2.3. Subsistemas que lo componen

En esta sección únicamente se hará mención de los subsistemas que componen al producto final, más adelante se detallará en capítulos el funcionamiento particular de cada uno de estos bloques.

- Nodo receptor
 - Microcontrolador STM32F103C8T6.
 - Receptor de RF.
 - Integrado para comunicación RS-485.
- Central de procesamiento
 - Microcontrolador STM32F103C8T6.
 - Integrado para comunicación GSM/GPRS.
 - Integrado para comunicación RS-485.

Capítulo 3

Nodos de recepción

3.1. Descripción general

En este capítulo haremos un análisis profundo sobre el funcionamiento de los nodos en el sistema de detección de inhibidores de alarma de autos. Para comenzar con el mismo es importante preguntarse: ¿qué funciones debe cumplir un nodo en el sistema? La respuesta a esto es evidente, en el nodo se producirá la recepción de la señal de RF mediante el módulo CC1101 de Texas Instruments, luego de esto la demodulación ASK efectuada por el receptor será procesada en el microcontrolador seleccionado para determinar si hay o no inhibición según estrategias más adelante detalladas y este se encargará de realizar la comunicación mediante el protocolo RS485 con la central de procesamientos. Integrado en el nodo se utilizan tres protocolos de comunicación: en primer lugar tenemos la comunicación SPI que se encarga de la interacción entre el microcontrolador y el receptor seleccionado; esta comunicación se utiliza para configurar los registros del CC1101 para establecer el modo de trabajo deseado. En segunda instancia tenemos comunicación serial asíncrona entre un pin de salida del receptor por el cual se mandan los datos RAW de demodulación en el canal seleccionado y en último lugar tenemos el protocolo RS485 para la comunicación de la red armada.

3.2. Prototipo

El proceso de obtener un sistema sólido y que responda a las necesidades planteadas llevó consigo la necesidad de elaborar dos modelos distintos



agregar imagen de nodo viejo

Para el diseño del esquemático nos hemos basado en las prestaciones que nos brinda el microcontrolador STM32F106C8T6. El mismo cuenta con comunicación SPI y serial integradas, por lo que haciendo uso del entorno de programación propio del fabricante (STM32 Cube IDE) hemos asignado los pines respectivos a cada comunicación, como se puede observar en la figura 3.1.



Trabajar con este entorno es muy beneficioso ya que facilita en algunos aspectos la configuración del microcontrolador seleccionado, teniendo la capacidad de, mediante una interfaz gráfica, activar comunicaciones, configurar los relojes, activar o desactivar interrupciones de timers y comunicaciones, entre otras.

Las interrupciones en nuestro diseño juegan un papel clave debido a que en la comunicación se ha optado en algunos casos particulares realizar el envío de los datos mediante interrupciones para que el procesador pueda continuar operando y no aboque todos sus recursos y tiempo de ejecución en enviar una palabra. De modo similar las interrupciones de timers nos han servido para realizar acciones con alta prioridad y que deben ejecutarse en un tiempo específico, como por ejemplo la lectura asíncrona de datos RAW enviados por un pin del CC1101. La configuración para las mismas se realiza de manera muy sencilla teniendo en cuenta la el contador de ticks del sistema, la frecuencia del clock utilizada y un preescaler a determinar para lograr el tiempo deseado.

3.3. Diseño final

El diseño el nodo ha surgido ciertas variaciones en el transcurso de la búsqueda del producto final. Entre estas se encuentra la optimización del PCB reduciendo el tamaño del mismo, retirar los indicadores led, dotar la placa con el integrado destinado a la comunicación (SN75176). Para hacer un análisis particular del funcionamiento del nodo hemos decidido analizar independientemente el software del hardware.

3.3.1. Software

El nodo al ser el encargado de recibir la señal de RF, demodularla y determinar si hay o no inhibición posee una alta carga de software desarrollado sobre él. De este modo señalaremos particularmente el desarrollo en cada uno de los siguientes aspectos.

- Recepción de RF.
- Estrategia de detección de inhibiciones.
- Comunicación con la central.



Recepción RF

El desarrollo de software en este aspecto cumple la necesidad que presenta el integrado receptor que utilizamos de ser configurado cada vez que este comienza a operar. Como previamente es analizado debemos establecer al dispositivo, que por características es un transceptor, en modo de recepción. Además se debe configurar la frecuencia de operación, el modo de demodulación, el tipo de salida de datos, entre otras muchas cosas que son cargadas en un total de 46 registros.

La carga de registros y el requerimiento de valor de RSSI que se le producen al CC1101 para tener noción de la potencia de RF en dBm que está llegando al receptor se realizan mediante comunicación SPI. Estos requerimientos son periódicos y han sido establecidos con un tiempo prudencial para que la comunicación resulte efectiva y los datos permanezcan actualizados.

Estrategia de detección de inhibiciones

La estrategia de detección de inhibiciones ha sido uno de los mayores desafíos a la hora de encarar el proyecto a causa de que el sistema debe ser confiable y robusto para poder instalarlo en una zona de operación y que no tenga fallos. Principalmente los errores de funcionamiento que son inadmisibles son:

- Falsas detecciones: que el sistema desate las alarmas cuando no hay presente un inhibidor o cuando en el canal se está comunicando un dispositivo que sí es apto para hacerlo, como por ejemplo una llave de auto.
- Falsos negativos: que el sistema sea incapaz de reconocer una señal que sea perjudicial para el sistema de seguridad de un automóvil.

Antes se ha profundizado en las estrategias de inhibición y se ha llegado a la conclusión de que existen dos métodos posibles para inhibir una comunicación, un método es saturación de la etapa receptora y el otro es por corrupción de la trama de datos. Para ambos métodos se ha debido realizar una estrategia de detección diferente, las cuales funcionan en simultáneo en el nodo para desatar las alertas correspondientes si detectaran positivo. A continuación en las figuras 3.3 y 3.2 se demuestra en bloques el funcionamiento de la estrategia de detección.

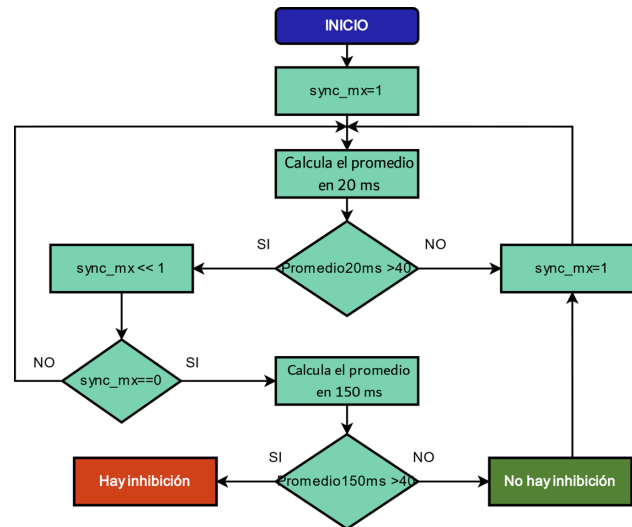


Figura 3.2: Estrategia de detección por corrupción de datos

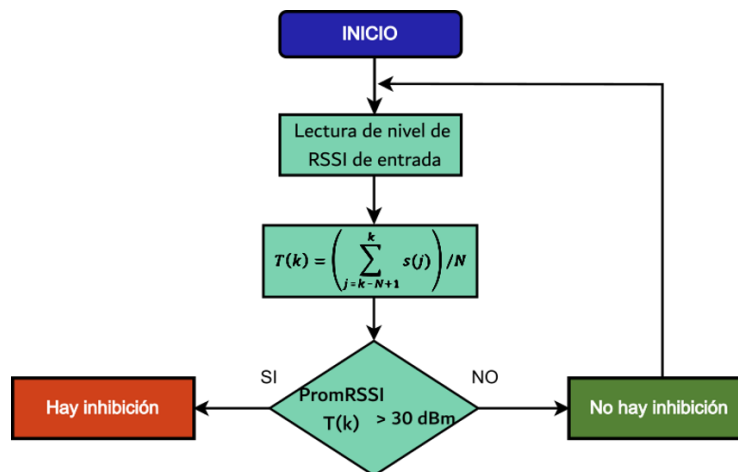


Figura 3.3: Estrategia de detección por saturación de etapa receptora

Capítulo 4

Desarrollo de servidor web

En este capítulo se describirán los objetivos, el diseño, las prestaciones y la forma en que se llevó a cabo el montaje del servidor web.

4.1. Objetivos

Los objetivos de tener un servidor web que disponga de una base de datos y una interfaz visual, como lo es la pagina web, son:

- Recabar la información brindada por cada lugar en donde se instale el sistema.
- Organizar todos los datos obtenidos en un solo lugar para que cada usuario tenga en forma remota y de fácil acceso las zonas donde se presentan este tipo de hechos.
- Mostrar en forma de tabla cada una de las inhibiciones detectadas.
- En base a esta tabla, generar diferentes gráficos que muestren de una forma mas amigable el texto plano.
- Tener un lugar de soporte/sugerencias.
- Procesamiento matemático para la triangulación y muestra gráfica de la última detección de un lugar de interés.



4.2. Página web

El dominio es <http://www.jammer-detector.ml> y la programación de la misma fue realizada en:

- HTML, siglas en inglés de HyperText Markup Language, hace referencia al lenguaje de marcado para la elaboración de páginas web. Es un estándar que sirve de referencia del software que conecta con la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código para la definición de contenido de una página web, como texto, imágenes, vídeos, scripts, entre otros. Es el estándar que se ha impuesto en la visualización de páginas web y es el que todos los navegadores actuales han adoptado.

El lenguaje HTML basa su filosofía de desarrollo en la diferenciación. Para añadir un elemento externo a la página (imagen, vídeo, script, entre otros.), este no se incrusta directamente en el código de la página, sino que se hace una referencia a la ubicación de dicho elemento mediante texto. De este modo, la página web contiene solamente texto mientras que recae en el navegador web (interpretador del código) la tarea de unir todos los elementos y visualizar la página final. Al ser un estándar, busca ser un lenguaje que permita que cualquier página web escrita en una determinada versión, pueda ser interpretada de la misma forma (estándar) por cualquier navegador web actualizado.

Es un lenguaje de marcado que nos permite indicar la estructura de nuestro documento mediante etiquetas. Este lenguaje nos ofrece una gran adaptabilidad, una estructuración lógica y es fácil de interpretar tanto por humanos como por máquinas.

- CSS (siglas en inglés de Cascading Style Sheets), en español "Hojas de estilo en cascada", es un lenguaje de diseño gráfico para definir y crear la presentación de un documento estructurado escrito en un lenguaje de marcado. Es muy usado para establecer el diseño visual de los documentos web, e interfaces de usuario escritas en HTML o XHTML. Junto con HTML y JavaScript, CSS es una tecnología usada por muchos sitios web para crear páginas visualmente atractivas, interfaces de usuario para aplicaciones web y GUIs para muchas aplicaciones móviles.



CSS está diseñado principalmente para marcar la separación del contenido del documento y la forma de presentación de este, características tales como las capas o layouts, los colores y las fuentes. Esta separación busca mejorar la accesibilidad del documento, proveer más flexibilidad y control en la especificación de características presentacionales, permitir que varios documentos HTML compartan un mismo estilo usando una sola hoja de estilos separada en un archivo .css, y reducir la complejidad y la repetición de código en la estructura del documento.

- PHP es un lenguaje de programación de uso general que se adapta especialmente al desarrollo de aplicaciones web dinámicas con acceso a información almacenada en una base de datos. El código fuente escrito en PHP es invisible al navegador web y al cliente, ya que es el servidor el que se encarga de ejecutar el código y enviar su resultado HTML al navegador.

Es libre, por lo que se presenta como una alternativa de fácil acceso para todos y además posee una amplia documentación en su sitio web oficial, entre la cual se destaca que todas las funciones del sistema están explicadas y ejemplificadas en un único archivo de ayuda.

- JavaScript (abreviado comúnmente JS) es un lenguaje de programación interpretado. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico.

Se utiliza principalmente del lado del cliente, implementado como parte de un navegador web permitiendo mejoras en la interfaz de usuario y páginas web dinámicas.

JavaScript se diseñó con una sintaxis similar a C, aunque adopta nombres y convenciones del lenguaje de programación Java.

Puntualmente la aplicación que se le dio en este proyecto es realizar operaciones matemáticas para la triangulación y únicamente en el marco de la aplicación cliente, sin acceso a funciones del servidor generar gráficas a partir de base de datos, previamente obtenidas mediante el lenguaje PHP.

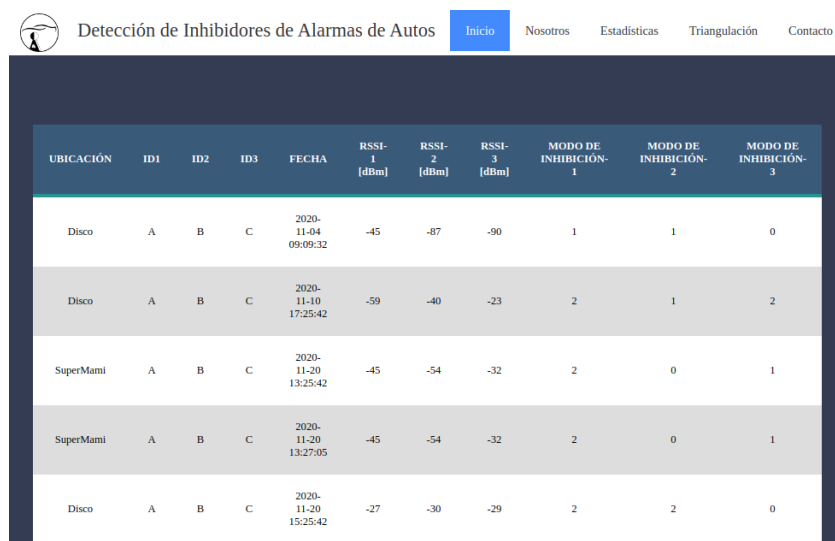


4.2.1. Pestañas

Inicio

Apenas ingresamos a la página podemos observar en la parte superior el logo y nombre del proyecto y sobre la misma barra en la parte derecha vemos el menú.

En esta pestaña de inicio se colocó la tabla donde muestra la información recabada de todos los lugares donde está instalado el sistema y se encontró una inhibición. La información que posee la misma es: ubicación, ID de cada nodo, fecha y hora y el nivel de RSSI y tipo de inhibición detectada por cada uno de los nodos. En la figura 4.1 podemos ver la misma.



The screenshot shows the 'Inicio' page of a web application titled 'Detección de Inhibidores de Alarmas de Autos'. The page features a navigation bar with links: Inicio (highlighted), Nosotros, Estadísticas, Triangulación, and Contacto. Below the navigation bar is a table with the following data:

UBICACIÓN	ID1	ID2	ID3	FECHA	RSSI-1 [dBm]	RSSI-2 [dBm]	RSSI-3 [dBm]	MODO DE INHIBICIÓN-1	MODO DE INHIBICIÓN-2	MODO DE INHIBICIÓN-3
Disco	A	B	C	2020-11-04 09:09:32	-45	-87	-90	1	1	0
Disco	A	B	C	2020-11-10 17:25:42	-59	-40	-23	2	1	2
SuperMami	A	B	C	2020-11-20 13:25:42	-45	-54	-32	2	0	1
SuperMami	A	B	C	2020-11-20 13:27:05	-45	-54	-32	2	0	1
Disco	A	B	C	2020-11-20 15:25:42	-27	-30	-29	2	2	0

Figura 4.1: Página de inicio

Nosotros

Esta pestaña está realizada para mostrar la tarjeta de cada uno de los integrantes del grupo de trabajo, dando así también un medio de contacto.

En la figura 4.1 podemos ver la pestaña.



Figura 4.2: Presentación de grupo de trabajo

Estadísticas

La sección de estadísticas, quizás la mas importante para los usuarios del sistema, es en donde, de una forma gráfica y amigable, se visualizan todos los datos representados por los gráficos que mas describan la situación.

En la figura 4.3, a la izquierda podemos ver un gráfico de torta con las formas de inhibiciones detectadas y a la derecha vemos un gráfico de barras que indica la cantidad de inhibiciones por cada lugar.



Figura 4.3: Gráficos de estadísticas



Triangulación

Esta sección está dedicada al procesamiento matemático y muestra de la triangulación de inhibiciones detectadas por corrupción de datos con baja potencia. En la figura 4.4 un círculo de un radio de 7 metros el cual nos indica la posición de la inhibición detectada.

El proceso matemático para el calculo de este punto se basa en la relación de potencia recibida y transmitida de una onda en el espacio libre, considerado así para la simplificación de cálculos, ecuación 4.1.

$$\frac{P_R}{P_T} = \left[\frac{4 * \pi * d_1}{\lambda} \right]^2 \quad (4.1)$$

Operando con la ecuación 4.1 para una misma señal recibida por dos nodos a la vez y haciendo la relación entre ellas obtenemos:

$$\left(\frac{d_1}{d_2} \right)^2 = 10^{\frac{P_d B m_2 - P_d B m_1}{10}} \quad (4.2)$$

$$\frac{d_1}{d_2} = 10^{\frac{P_d B m_2 - P_d B m_1}{20}} \quad (4.3)$$

Esta relación de distancias nos establece un punto en la recta que une cada nodo entre si (estos se encuentran en los vértices del triangulo azul como se ve en la figura 4.4), del cual trazando una linea perpendicular a ella, tenemos la linea de acción del inhibidor.

Haciendo esta relación entre todos los nodos tenemos 3 lineas que conforman un triángulo por la intersección entre ellas, donde luego obtiene la intersección de dos de las mediatrices de estas rectas que nos determinan el centro de la circunferencia que une los 3 puntos encontrados. El punto central, con un radio de 8 metros es el área donde se encuentra la inhibición detectada.

Contacto

Finalmente la última pestaña es la de contacto, la cual tiene el fin de que cualquier persona que entre a la página y tenga alguna duda o sugerencia pueda tener un contacto rápido con cada uno de nosotros (figura 4.5).

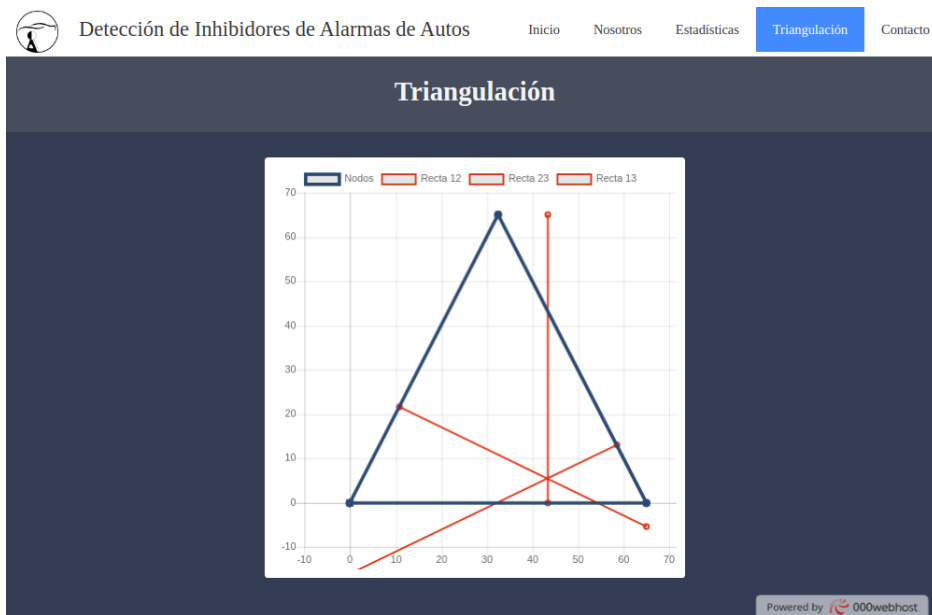


Figura 4.4: Pestaña de triangulación

Figura 4.5: Formulario de contacto



4.3. Base de datos

La base de datos esta realizada y gestionada en phpMySQL y cuenta con una tabla con el mismo contenido que la que podemos ver en la figura 4.1.

Es el lugar en el cual se almacena cada inhibición detectada y luego, mediante un enlace con la página web, todo su contenido es visualizado en esta la misma.

4.3.1. Carga de datos

El enlace desde el servidor web con la central instalada en cada lugar se realiza mediante el acceso a una pestaña oculta de la web, en la cual se interactúa con la central mediante un algoritmo de http-POST-request para cargar cada uno de los datos de los nodos correspondientes a cada lugar, para luego procesarlos y obtener los gráficos ya mencionados, la triangulación en caso de ser posible y otras utilidades que se le puedan dar.

Capítulo 5

Conclusiones y trabajo futuro

De acuerdo al trabajo previamente expuesto en este capítulo haremos mención de las conclusiones que pudimos extraer al finalizarlo y se evaluarán posibilidades de desarrollos futuros.

5.1. Conclusiones

En primera instancia nos parece importante dar nuestra perspectiva respecto a la viabilidad del proyecto. El mismo fue enfocado con carácter de costos minimizados buscando que el uso de los recursos monetarios disponibles sea el más eficiente posible. De esta manera nos encontramos con un producto finalizado que luce muy adecuado para la fabricación en cantidad aunque se reconoce que la utilización de módulos prefabricados -como previamente se analiza- es muy beneficiosa para la producción de los prototipos y primeros sistemas, pero en la posibilidad de producir en serie debería hacerse una adaptación de esto a un sistema que integre todo los bloques en fabricación propia. En las primeras instancias de fabricación se observa que muchos de los componentes utilizados precisan ser importados y, debido a la situación actual del país y a la alta carga impositiva que esto implica, resulta no ser conveniente la compra de un pequeño número de dispositivos en el exterior, quedando así avalado el uso de algunos bloques componentes.

Desde el punto de vista económico el sistema planteado cuenta con un punto débil el cual está definido en los requerimientos del mismo. Se busca que el sistema de seguridad no pueda ser inhibido por un agente externo por lo que los nodos y la central se comunican entre sí de manera cableada.



Resulta ser que el cableado debe ser de calidad que asegure la comunicación RS485 y en el mismo la alimentación para los nodos. Es por esto que en la aplicación del sistema planteado la mayor cantidad de gastos reside en las tiradas de cable necesarias para emplazar el sistema en el lugar de operación. Esto podría solucionarse con una metodología de comunicación inalámbrica pero daría lugar a altas vulnerabilidades.

La seguridad en la detección de inhibiciones en sistemas de seguridad de alarma de auto fue el eje central del desarrollo, por lo que siempre se buscó eliminar las vulnerabilidades que pudieran ocurrir. Es por esto que al momento de presentar el sistema podemos decir que posee un sistema de detección robusto. Las pruebas de campo han sido muy variadas y han buscado eliminar cualquier falla en el funcionamiento, ahora restaría el realizar un análisis en largo plazo de operación con una realimentación del cliente que fuera a utilizarlo.

Como cierre, podemos decir que se ha conseguido un sistema que es capaz de detectar en fracciones de segundos señales que alteren el funcionamiento de seguridad inalámbricos en la frecuencia de 433,92 MHz. El área de operación segura para que las señales de baja potencia puedan ser trianguladas se estima que es de 50m a la redonda desde el punto central de una disposición en forma triangular de los tres nodos, de igual modo esto podría ser ampliado con la penalización de que no todos los nodos en simultáneo alcancen a medir un valor de intensidad de señal en una inhibición por corrupción de datos.

5.2. Trabajo futuro

Después de terminar el trabajo enmarcado en el proyecto final de grado de ingeniería electrónica hemos podido divisar algunos puntos sobre los cuales nos parece importante realizar mejoras en un futuro:

- Frecuencia de operación: nuestro sistema fue diseñado para una única frecuencia de operación; como previamente fue expuesto existen dos principales en las que funcionan los receptores vehiculares, por lo que a futuro creemos importante que el sistema tenga la capacidad de detectar en ambas las inhibiciones presentes.
- Las inhibiciones y las estrategias de inhibición son diferentes para cada sistema de comunicación, por lo que creemos interesante evaluar la posibilidad de detectar inhibiciones en diversos sistemas, aplicando e



investigando sobre métodos para determinar las inhibiciones particularmente para cada comunicación.

- El sistema de detección fue elaborado con tres nodos distribuidos espacialmente para tener la capacidad de predecir la procedencia de la señal. En nuestros planes cabe la posibilidad de desarrollar un sistema único portable que detecte inhibiciones a su alrededor, dando lugar a la venta de un producto para particulares. Este debería disponer de alarmas locales y un sistema de memoria de datos recolectados que puedan ser descargados por el usuario.
- Como antes fue mencionado es importante que en un futuro el diseño del sistema sea completamente integrado a una placa única, esto nos daría la posibilidad de reducir los tamaños y tener un sistema más redituable para ventas en cantidad.