SPECTRUMSENS

Detecta, analiza, monitoriza y actúa

Protección exterior e interior (RF - Inteligencia de datos)

Jordi Garcia Castillón – info@jordigarcia.eu – Tel. (+34) 636714253

Síntesis

Desarrollo de un analizador de espectro pensado sobre todo para el ámbito empresarial (aunque también doméstico) que tiene como objetivo el realizar una monitorización permanente del entorno del espectro RF del cliente para informarle y, llegado el caso, protegerle de potenciales interferencias por ataques cibernéticos de su entorno inalámbrico malintencionados.

El dispositivo realizará una monitorización constante modulable (habitualmente dentro de un rango que irá entre los 30 kHz y los 30 GHz, rango y bandas que podrán ser perfiladas según el ámbito geográfico donde deba de rendir servicio el dispositivo).

El objetivo prioritario será el de realizar el patronaje de los comportamientos habituales, especialmente en las bandas de espectro que pueden tener una implicación directa con el funcionamiento de los dispositivos y mecanismos del entorno inalámbrico a proteger.

Las principales bandas por proteger serán todas aquellas relacionadas con los dispositivos que pueden funcionar dentro del rango de las bandas ISM, banda para usos de RFID, bandas WiFi, banda para usos de bluetooth y todas las bandas asignadas a los usos de telefonía móvil de uso convencional, entre otras.

En caso de detectar anomalías en el espectro analizado, el dispositivo será capaz de emitir una señal indicando la anomalía para su análisis. A partir de este punto, el sistema será escalable pudiendo incorporar lo siguiente:

- Sistema de envío de los datos registrados a un aplicativo externo o bien a un aplicativo expresamente diseñado para cada cliente para su uso de monitoreo exclusivo

- Sistema de respuesta mediante la emisión de una señal de mayor alcance a la percibida como potencialmente anómala para intentar neutralizar los efectos de esta (sólo activo en aquellas jurisdicciones en las que esta funcionalidad pueda resultar plenamente legal). En el caso de aquellos entornos donde la funcionalidad no resulte legal se podrá realizar una automatización *shutdown* de todos los dispositivos que estén actuando en las frecuencias afectadas

- Capa de servicio proporcionada al cliente que monitorice por él su espectro RF en modo 24 x 7 x 365 y, en caso de anomalía, le alerte y actúe de ser necesario

Todo lo anterior acompañado de una capa integral de servicios que incluirá:

- Negocio en capa de servicio (capacitación, auditorías, implementaciones, central de alarmas de eventos y gestión de éstas, etc.)

- Negocio en desarrollos personalizados (hardware IoT, software de control, etc.).

Y con el desarrollo opcional paralelo, pero integrado, de una plataforma de inteligencia de datos basada en la acumulación y análisis de datos individualizados para cada cliente en base a sus eventos de seguridad (del entorno RF y otros) de sus dispositivos que desemboquen en una plataforma "IntelligenSys" autogestionada por el cliente o gestionada externamente como capa de servicio.

A modo de resumen de la solución ofrecida a los usuarios destinatarios indicar lo siguiente:

- Cúpula de seguridad de doble nivel: interno y externo

- Base homogénea con alta capacidad de personalización

- Solución multiparadigma: hardware y software

- La base de hardware estandarizado puede plantearse, en la medida de lo posible, como open source para su investigación y desarrollo constante y, desde ese punto, desembocar en los servicios asociados y los proyectos cerrados personalizados modulares y personalizados

DESARROLLO TÉCNICO

Desarrollo técnico de base sobre el cual se estructurará todo el desarrollo modular

RESUMEN

El propósito general de este desarrollo es establecer la base abierta de un sistema que, posteriormente, se podrá modular según las necesidades concretas de cada parte usuaria y adaptando el rango de frecuencia o de frecuencias a cada ámbito concreto, así como su desarrollo específico.

A partir de esta base abierta se puede desarrollar una comunidad, así como un sistema de investigación y de desarrollo que redunde en un beneficio conjunto para el entorno RF general y que ello aporte soluciones particulares a situaciones y casos concretos.

En este caso, a modo de ejemplo introductorio, se trabajará sobre la base de una única frecuencia de 700 MHz y en un sistema que pueda funcionar de forma autónoma (modo *standalone*) y, a partir de dicha base, se pueden introducir capas de integración conectada, así como elementos de precisión y de desarrollo específicos.

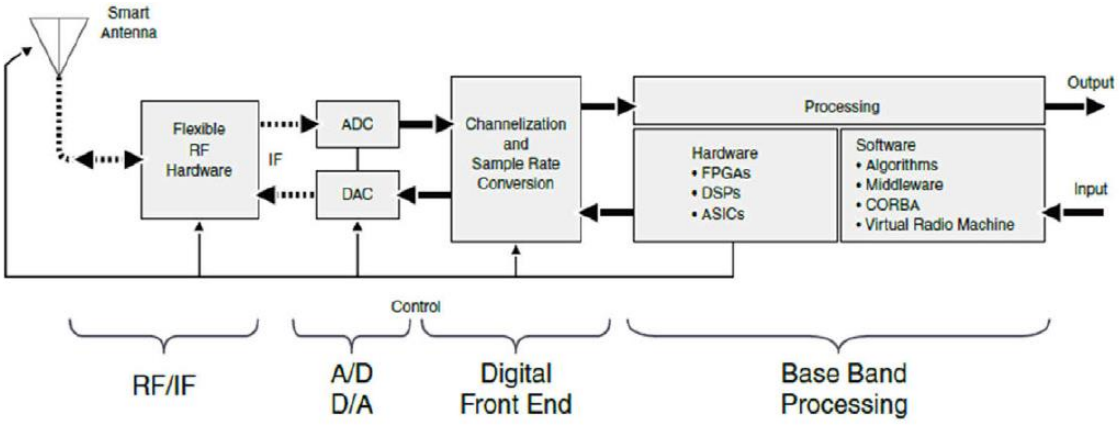
El objetivo del desarrollo de la base es establecerla sobre sistemas abiertos como pueden ser microcontroladores / microprocesadores como ARDUINO o RASPBERRY por poner dos ejemplos.

Aunque son distintas las opciones posibles (del mismo modo que son distintas las posibilidades de conectividad posterior a plataformas de visualización o de alertas, así como a redes: SIGFOX, LORA, etc.), en este caso, se escoge concretamente a Raspberry Pi, ya no tan sólo por el bajo coste del desarrollo, sino por la capacidad de operar con un sistema SDR con receptor RTL-SDR.

Este sistema de base (en general aplica a todo el “entorno IoT” e “ISM clásico”) permite obtener un sistema autónomo que es capaz de detectar transmisiones indeseadas que se encuentren en el estándar IEEE 802.11g/b/n/ac. En este caso, por las propias restricciones del sistema empleado, la banda de frecuencias que se pueden emplear serán las que van entre los 26 y los 1766 MHz, pero esta base permite que estableciendo ligeras variaciones se pueda trabajar sobre cualquier otra banda/s de espectro.

SDR (RADIO DEFINIDA POR SOFTWARE)

Uno de los grandes pilares de la base es la Radio Definida por Software (SDR) y debemos entender a la misma, para el caso que aquí nos ocupa, en base a su esquema general:



Conceptualmente, podemos decir que una SDR dispone de un apartado RF (antena, filtros, amplificadores, etc.), un ADC (conversor de señal analógica a digital) o DAC (conversor de señal digital a analógica) y de un *digital front end*.

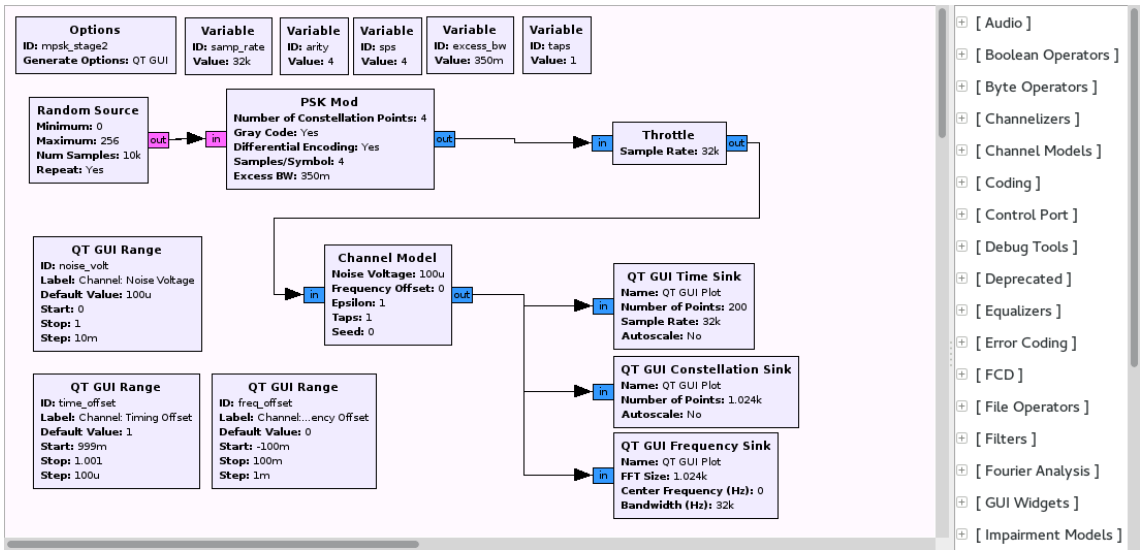
Un sistema SDR ofrece claras ventajas como son la simplificación de los procesos de desarrollo de aplicativos, pues permite hacerlo mediante líneas de código sin tener que realizar modificaciones físicas en los elementos hardware. También permite un sistema flexible llegado el momento de modificarlo. A su vez, es fácil de actualizar y su coste no es elevado.

Uno de los aspectos esenciales del funcionamiento del SDR se encuentra en la fase de conversión de la señal de digital a analógica. Esta etapa resultará determinante pues de la misma se desprenden los límites del ancho de banda que tendrá el sistema y ello será en base al conocido popularmente como Teorema de Nyquist.

En dicho teorema queda establecida la condición que debe cumplirse en el muestreo de señal para que dicha señal pueda ser recuperada sin pérdidas:

$$f_s > 2 * f_{max} = 2 * B$$

Para controlar un sistema de radio y realizar el tratamiento de la señal se empleará el software GNU radio basado en bloques. Del mismo podemos ver una representación gráfica a continuación:

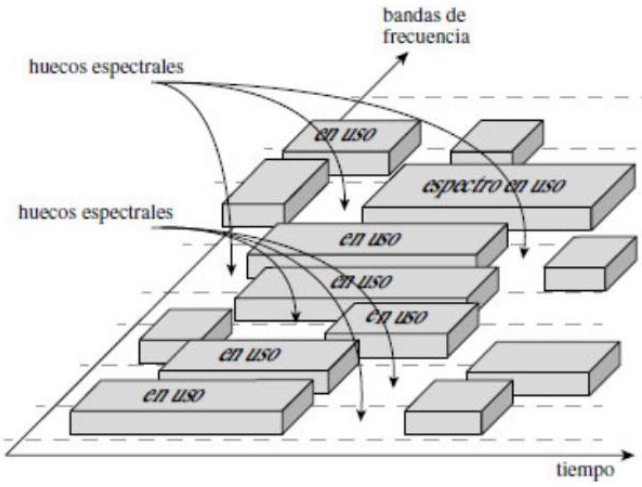


Puede decirse que, actualmente, los sistemas SDR tienen un alto nivel de aplicación en el ámbito empresarial y también militar. Las aplicaciones pueden resultar distintas, su desarrollo y uso se encuentra en plena expansión, el desarrollo de soluciones de bajo coste como las aquí planteadas contribuyen a expandirlo y consiguen que los mismos puedan acabar llegando a todas las capas de la sociedad para su uso (mitigando la "*commoditization*" mediante la capa de servicio, capa que a la postre es la que garantiza la especificidad y la evolución constante del negocio a ella adscrito).

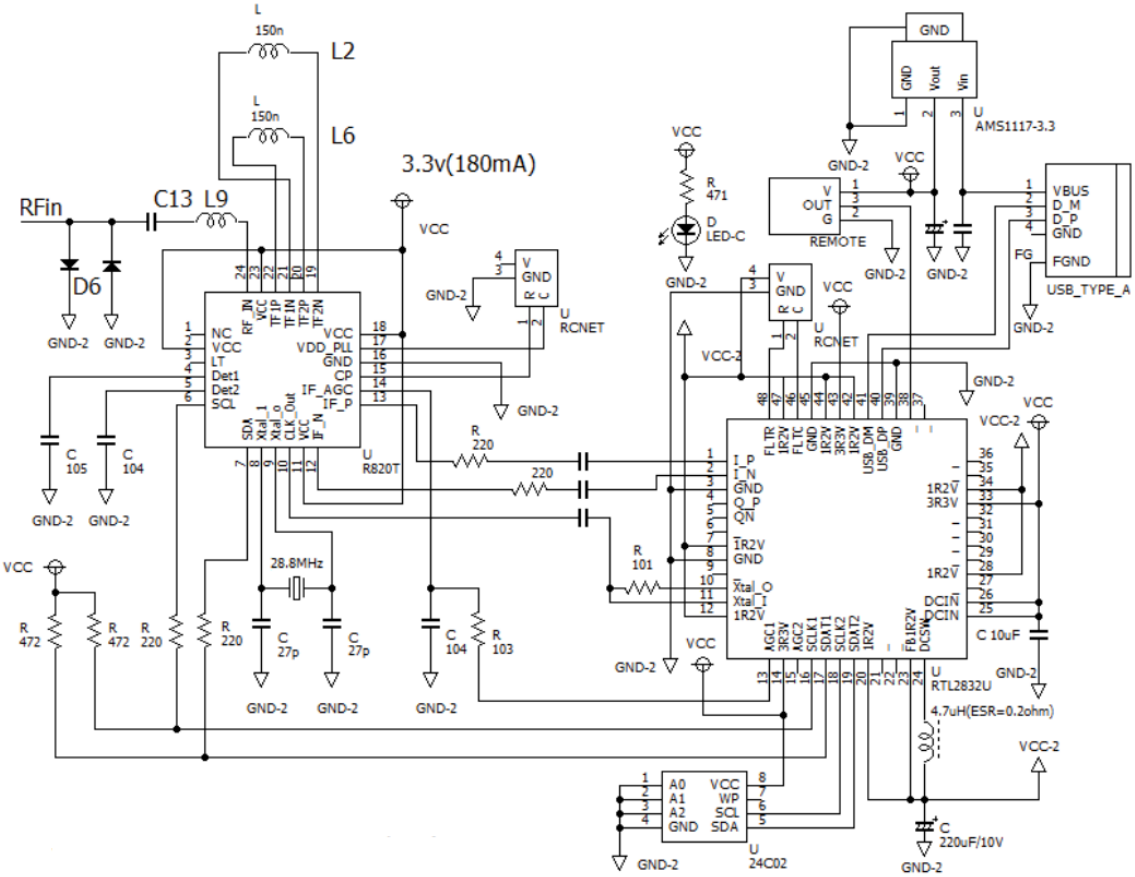
La expansión de los sistemas SDR y su evolución debe llevar a trabajar en la investigación y desarrollo de mayores capas de respuesta activa. Entre estas capas se puede encontrar la de la acción de "ataque contra ataque" (como la que dentro de este sistema se plantea cuando la legislación lo permite), pero una opción menos "agresiva" se encuentra en la radio cognitiva, ya que la misma pretende y permite sortear en gran parte los sistemas de agresión intencionada o interferencias y situaciones de saturación o colapso general.

La radio cognitiva no tiene la función de intentar neutralizar un ataque lanzando otro ataque, sino que pretende esquivar el ataque mediante su movimiento táctico a otras frecuencias no atacadas, interferidas u ocupadas. En realidad, nos podríamos encontrar en un escenario donde todas las frecuencias estén siendo atacadas, en tal caso lo ideal sería (siempre que la legislación del lugar lo permita) en todo caso una solución híbrida que sería la implementación combinada de un sistema de radio cognitiva con un sistema de *jamming* destinado a realizar funciones de *antijamming, un shutdown o un "enjaulado" robusto global*.

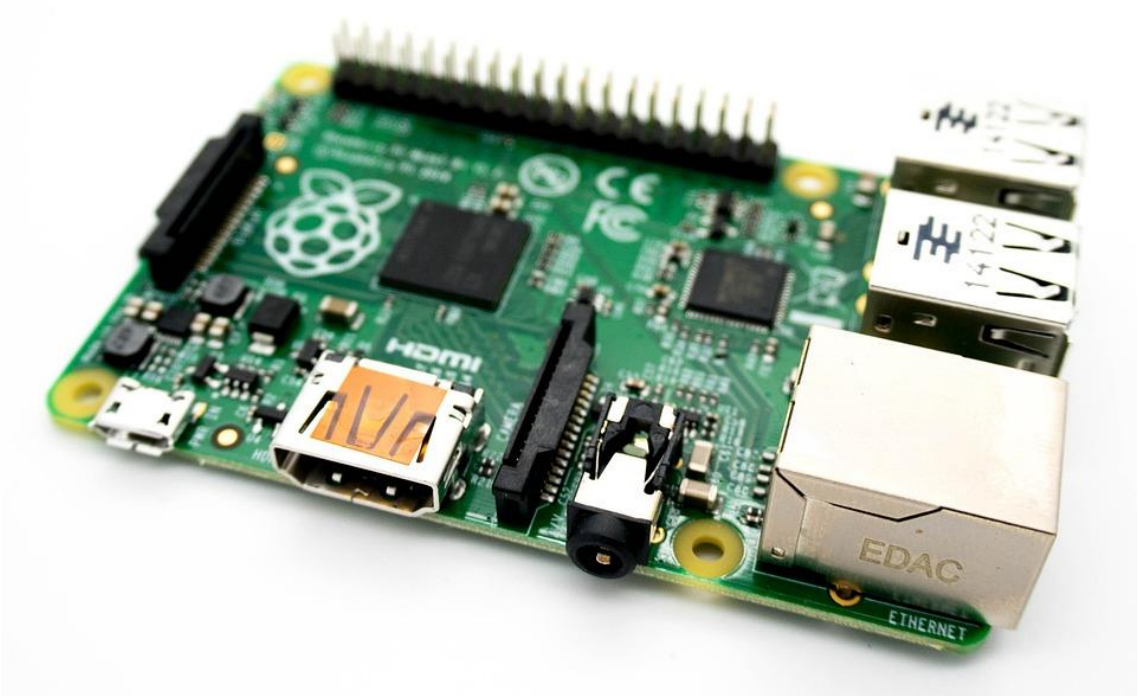
Un ejemplo gráfico de un sistema de esquema de radio cognitiva puede encontrarse a continuación:



Y todo ello partiendo de un esquema RTL-SDR eléctrico general:



Para este desarrollo base quien se encargará de controlar el receptor RTL-SDR y de realizar el procesado de las señales que se obtengan será, tal y como ya se ha mencionado, una Raspberry Pi. Concretamente se tratará de su versión 3 modelo B):



Algunas de sus especificaciones técnicas principales de esta versión y modelo son las siguientes:

Procesador:

Chipset Broadcom BCM2387

1,2 GHz de cuatro núcleos ARM Cortex-A53

GPU:

Dual Core VideoCore IV ® Multimedia Coprocesador. Proporciona Open GL ES 2.0, OpenVG acelerado por hardware y 1080p30 H.264 de alto perfil de decodificación

Capaz de 1 Gpixel / s, 1.5Gtexel / s o 24 GFLOPs con el filtrado de texturas y la infraestructura DMA

RAM:

1GB LPDDR2

Conectividad:

Ethernet socket Ethernet 10/100 BaseT

802.11 b / g / n LAN inalámbrica y Bluetooth 4.1 (Classic Bluetooth y LE)

Salida de vídeo

HDMI rev 1.3 y 1.4

RCA compuesto (PAL y NTSC)

Salida de audio

Jack de 3,5 mm de salida de audio

USB 4 x Conector USB 2.0

Conector GPIO

40-clavijas de 2,54 mm (100 milésimas de pulgada) de expansión: 2x20 tira

Proporcionar 27 pines GPIO, así como 3,3 V, +5 V y GND líneas de suministro

Conector de la cámara de 15 pines cámara MIPI interfaz en serie (CSI-2)

Pantalla de visualización. Conector de la interfaz de serie (DSI). Conector de 15 vías plana flex cable con dos carriles de datos y un carril de reloj

Ranura de tarjeta de memoria “empuje/tire” microSD

El sistema que será empleado para este desarrollo base será el S.O Raspbian Jessie Lite. Dicho sistema operativo tiene su base en Linux Debian. En este caso, el mismo no dispondrá de interfaz gráfica y se ejecutará de forma directa sobre una tarjeta microSD sin necesidad de disco duro.

Siempre hablando del desarrollo base, éste se llevará a cabo mediante la habilitación del servidor SSH para la creación de un túnel para el manejo remoto desde otra computadora.

Para la realización del testeo y depuración para la observación de la zona del espectro que va a ser analizado de forma constante y en tiempo real se utilizará SIMULINK / MATLAB.

La programación principal aquí planteada se realiza en C. Todo ello mediante el empaquetado con CMake.

Se utilizarán los programas “rtl-sdr.c” de Osmocom y también el programa “rtl_power” también programado en C. El primero resultará adaptado y el segundo será el encargado de realizar la medición de amplios anchos de banda espectrales.

Aunque existen muy variadas opciones para implementar el envío y mostrado de las alertas que se produzcan (y en cada caso particular se podrá analizar la mejor para cada situación en concreto) en este desarrollo base se realizará mediante el *framework* Node.js.

Concretamente, se desarrollará una aplicación cliente que será ejecutada en la Raspberry Pi conectada a red y un pequeño servidor en un host que cuente con conexión a Internet y que disponga de una IP fija.

La conexión entre el cliente y el servidor se realizará mediante la utilización de un socket TCP. Un pequeño resumen de la arquitectura de esta capa de red sería el siguiente:

ENTORNOS DE VALIDACIÓN

Para validar la aplicación de dicho sistema base corresponde poner el ejemplo de éste en 2 escenarios diferentes, con unas particularidades concretas en cuanto a recepción de señales RF se refiere y que responden a 2 escenarios comunes para todas las empresas, particulares, etc.:

A) Entorno 1: dispositivo funcionando en un entorno "semitransparente". Eso es en un espacio o elemento externo o en un edificio cualquiera con una ligera cubierta pero que permite la entrada y salida de señales RF con buen nivel de señal. Este es el caso típico de la mayoría de las oficinas, naves industriales, domicilios particulares, etc.

B) Entorno 2: dispositivo funcionando en un entorno "opaco". Esto es en un edificio con elementos estructurales que no limitan del todo la conectividad pero que la reducen al máximo, en entornos soterrados, etc.

En ambos casos:

1- La monitorización se realiza de forma continua sobre la banda de 700 MHz y se realiza una verificación del envío de alarmas

2- El dispositivo trabaja de forma autónoma mediante batería externa.

3- El dispositivo tiene como objetivo el captar la señal o señales (esto resultaría extensible a todos los rangos de frecuencia que se desee) que se estén emitiendo dentro de su rango de alcance, monitorizar la/s misma/s y emitir señales de alerta cuando las emisiones existentes cambien de potencia según unos parámetros porcentuales señalados o cuando capte nuevas emisiones dentro del rango (pudiendo establecer bandas de exclusión con la finalidad de evitar falsos positivos). El sistema puede utilizar el aprendizaje automático para "aprender" y "evolucionar" por sí mismo sobre las señales del entorno fijo que se encargará de analizar a lo largo de su vida útil

Esquema global del sistema hardware base: