

# Desarrollo de un sistema de exploración OFF-LINE del espectro radioeléctrico, basado en el análisis de datos goniométricos.

**Autor:** Rey Alameda, Javier

**Director:** Nuñez Ortuño, José María

Contacto: jreyala@et.mde.es

---

**Resumen:** Actualmente, la exploración del espectro radioeléctrico con la finalidad de escuchar, interceptar y localizar emisiones radioeléctricas de interés, se realiza en base a receptores de banda ancha, los cuales de una manera ON-LINE presentan la actividad existente en tiempo real. Esto supone que, aquellas emisiones que no se traten en el preciso momento de su interceptación, se perderá su información, a no ser, que puedan ser tratadas a posteriori.

Igualmente, no existe un sistema que posibilite el análisis del comportamiento en el tiempo de esas emisiones captadas.

Por estos motivos y basado en la información goniométrica proporcionada por un sistema de guerra electrónica (EW), este trabajo pretende implantar las bases de un modelo de sistema que posibilite:

- Almacenar la información goniométrica proporcionada por un sistema de EW, en un ancho de banda determinado, así como en un margen de tiempo.
- Poder llevar a cabo un análisis de manera conjunta (tiempo y frecuencia de emisión) para convertir orígenes de datos goniométricos, sin relación entre si, en información coherente, interactiva y atractiva visualmente.
- Mostrar la información goniométrica que se determine en un Sistema de Información Geográfica (GIS).
- Posibilitar en el contexto radioeléctrico y en base al análisis de BIG DATA de captaciones radioeléctricas, la realización de MACHINE LEARNING para detección de anomalías.

**Palabras clave:** Guerra electrónica (EW), sistemas de radiogoniometría, Big Data, Machine Learning, detección de anomalías.

---

## 1. Introducción

### 1.1. EW

La guerra electrónica (abreviado, EW, del inglés Electronic Warfare) [4] consiste en una actividad tecnológica y electrónica con el fin de determinar, explotar, reducir o impedir el uso

hostil de todos los espectros de energía, por ejemplo el electromagnético, por parte del adversario y a la vez conservar la utilización de dicho espectro en beneficio propio.

Dada la complejidad de las operaciones militares, la EW se divide en tres partes elementales:

- Medidas de apoyo de Guerra Electrónica (ESM).
- Contramedidas electrónicas (ECM).
- Medidas de Protección Electrónicas (EPM).

Las que nos interesan son las medidas ESM. Son actividades encaminadas a buscar, interceptar e identificar las emisiones electromagnéticas, así como a localizar su procedencia. La finalidad de estas actividades es la obtención de conocimiento acerca de la situación electromagnética (Orden de Batalla Electrónico OBE), y el reconocimiento inmediato de la amenaza. Dada su naturaleza, la ESM comparte muchas características comunes con las actividades realizadas para la obtención de inteligencia. Dichas actividades se suelen clasificar en las siguientes categorías: – Inteligencia de comunicaciones o COMINT (Communications Intelligence), consiste en la obtención de información a partir de las emisiones realizadas por sistemas de comunicaciones. – Inteligencia electrónica o ELINT (Electronic Intelligence), comprende las actividades dirigidas a obtener información técnica y de inteligencia a partir de emisiones realizadas por sistemas de no-comunicaciones (radares, perturbadores, etc.). – Inteligencia de señales o SIGINT, (Signals Intelligence), agrupa a COMINT y a ELINT. Se utiliza este término cuando no se quiere distinguir entre las dos. Dada su naturaleza, las actividades ESM comparten muchas características con las actividades SIGINT, siendo la principal diferencia entre ambas su finalidad y el uso que se haga de la información obtenida (apoyo a decisiones tácticas a corto plazo (ESM), o a decisiones estratégicas a largo plazo (SIGINT)).

Técnicas ESM [6]. Se puede generalizar que un sistema ESM realiza todas o parte de las siguientes tareas:

- **Exploración.** Utilizando sensores que captan las señales del entorno electromagnético. Los sensores constan de equipos receptores y antenas. Normalmente se dispone de receptores de banda ancha que cubren o exploran a gran velocidad un margen más o menos amplio del espectro, con el fin de detectar actividad en él.
- Interceptación. Cuando, durante la fase de exploración, se descubre una frecuencia que está emitiendo, pudiéndose grabar su frecuencia o no.
- Medida de parámetros. Los parámetros de los pulsos (señales de no comunicaciones) y de las señales de comunicaciones son medidos y digitalizados para su proceso posterior.
- Análisis y clasificación. Mediante hardware y software específico se analizan las señales captadas identificando sus parámetros técnicos, y se clasifican. En el caso de las transmisiones de comunicaciones digitales, se utilizan equipos para decodificarlas. El contenido de las comunicaciones se obtiene mediante operadores humanos, o bien mediante sistemas automáticos de reconocimiento del habla.
- Registro. Las señales captadas pueden ser registradas mediante equipos de grabación para su conservación o análisis posterior en laboratorio (**off-line**).

- Identificación. En equipos ESM de no comunicaciones, reuniendo los datos obtenidos del análisis de las señales se realiza una identificación automática o asistida por el operador. En sistemas ESM de comunicaciones se utilizan los datos del análisis de señal, el contenido de las transmisiones de comunicaciones, y la localización de los emisores para realizar una identificación de emisores basado principalmente en la experiencia del operador. Se apoyan en bases de datos obtenidas y depuradas mediante captaciones anteriores a lo largo de tiempo.
- Localización. Se utilizan equipos que permiten obtener de forma más o menos precisa la localización geográfica del emisor. Se consigue mediante radiogoniómetros, que son receptores capaces de determinar el ángulo de llegada de la señal. Utilizando varios de esos equipos situados en localizaciones suficientemente separadas, o bien un único equipo en movimiento, se puede obtener la localización por triangulación. También, existen sistemas que, para ciertos casos, además del ángulo en azimut determinan también el ángulo de elevación. Con ellos se puede obtener, en determinadas circunstancias, la localización utilizando un solo sensor.

Esta localización se basa en la radiogoniometría, cada vez más utilizada, ya que con las nuevas técnicas de transmisión de espectro ensanchado, es casi imposible conocer el contenido de la información transmitida, pero, gracias a la radiogoniometría, se puede conocer la fuente de origen de la emisión. La principal técnica de radiogoniometría utilizada, suele ser la interferometría. El principio básico del interferómetro correlativo consiste en comparar las diferencias de fase medidas, con las diferencias de fase obtenidas por el sistema, utilizando un ángulo de onda conocido. La comparación se realiza calculando el error cuadrático o el coeficiente de correlación de los dos conjuntos de datos.

## 2. Desarrollo

La primera necesidad que nos surge es la de tratar la ingente cantidad de señales radioeléctricas y goniometrías recibidas (BIG DATA), a posteriori de su recepción (**off-line**), en una base de datos ágil que permita a un usuario analizar esa cantidad de información basándose en alarmas y logs que detectarán el cambio de patrón seguido por las señales durante un determinado tiempo de muestreo.

Para el tratamiento, filtrado y representación de resultados se puede utilizar una herramienta de análisis de datos comercial que pueda manejar la ingente cantidad de datos de salida (BIG DATA). El análisis de datos es un proceso que consiste en inspeccionar, limpiar y transformar datos con el objetivo de resaltar información útil, para sugerir conclusiones y apoyo en la toma de decisiones. Se centra en la inferencia estadística, la cual permite tomar una decisión de forma sencilla con un grado de confianza determinado, identificando, analizando tanto datos como patrones de comportamiento.

Habría que crear una herramienta "ad-hoc" que analice los datos para proporcionar visualizaciones interactivas y poder crear sus usuarios informes y paneles. A falta de esa herramienta particular, se ha adoptado y "customizado" la herramienta POWER BI. Se necesitan que las máquinas sean capaces de realizar una variedad de acciones que no están implementadas en esta herramienta como: avisar cuando, entre una ingente cantidad de datos, alguno o algunos de ellos se salgan de la norma, es decir, cuando los datos entrantes sean diferentes a los patrones considerados normales. Se necesita un programa que establezca unas alarmas cuando:

- Exista un incremento o disminución anormal de emisiones en el éter,
- Cuando una plataforma emisora haya cambiado de azimut,
- Cuando haya habido un cambio en las horas de emisión de una plataforma conocida,

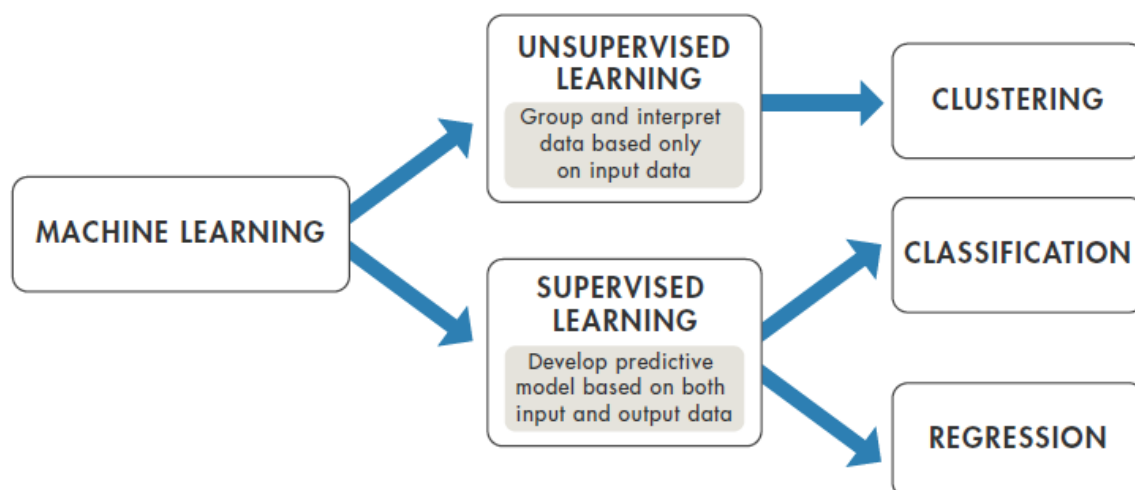
- Cuando una plataforma conocida cambie de frecuencia de emisión,
- Etc.

Para ello se necesita dotar al **sistema de exploración off-line**, de una herramienta de detección de anomalías basada en inteligencia artificial (IA) y más concretamente en la técnica "MACHINE LEARNING".

Machine learning[2] utiliza dos (2) tipos de técnicas, figura 1:

- Aprendizaje supervisado, el cual desarrolla modelos predictivos basados en datos conocidos de entrada y salida.
- Aprendizaje no supervisado, donde los datos se agrupan y se interpretan basándose solamente en los datos de entrada.

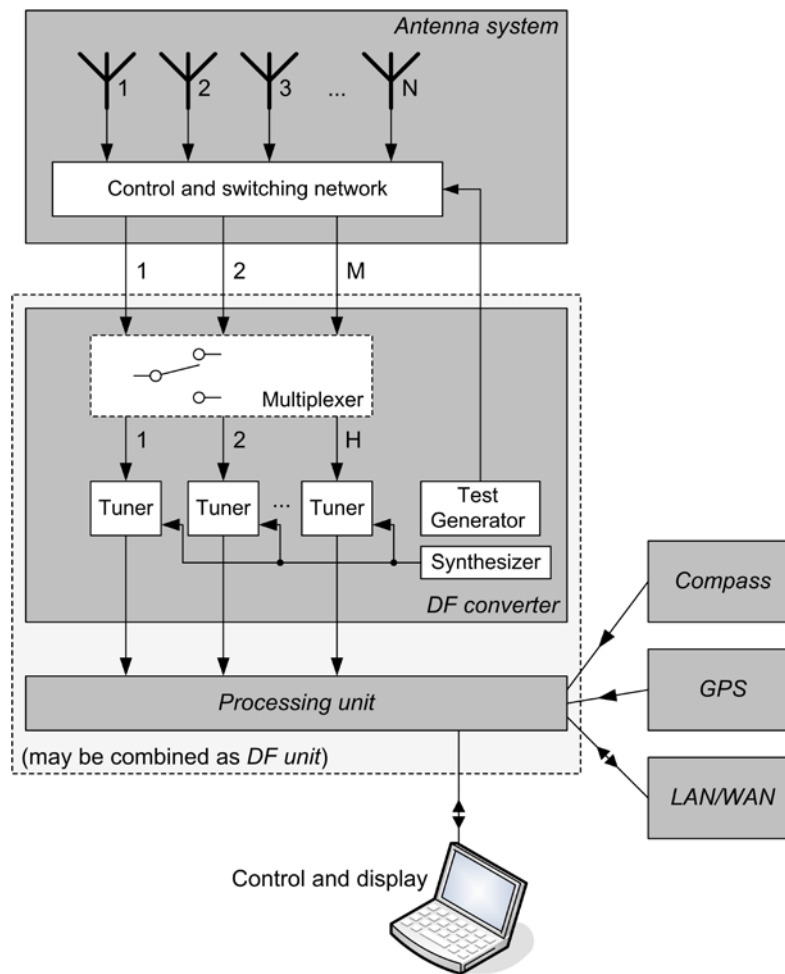
El algoritmo usado en el aprendizaje no supervisado se utiliza para analizar los datos conocidos y ser capaz de encontrar patrones escondidos. Los algoritmos de detección de anomalías no supervisadas sirven para detectar anomalías. Esta detección de anomalías no deja de ser una técnica de minería de datos que permite el reconocimiento de nuevos patrones con comportamiento inusual, los cuales pueden ser traducidos como acciones no válidas o anómalas sobre los datos.



**Figura 1.** División de tipos de aprendizaje y algoritmos.

### 3. Resultados y discusión

Los sistemas actuales de EW [1] están formados por una base goniométrica, es decir, conjunto de sensoras (varias antenas receptoras omnidireccionales distantes geográficamente entre si), que junto con un SW de tratamiento de señal y presentación, permiten a los operadores **explorar** el espectro electromagnético para detectar una emisión, figura 2-1, y localizarla utilizando el método de radiogoniometría descrito anteriormente (interferometría).



**Figura 2.** Componentes de un sistema de radiogoniometría (figura tomada de R&S DDF550 manual)

Para crear un sistema flexible y rápido se debería trabajar la selección de los datos en origen, en cada goniómetro utilizado, de tal forma que mediante una serie de algoritmos se extraigan los datos de interés según las misiones designadas.

El sistema debería constar de tres (3) diferentes Bases de Datos (BBDD). La BBDD de Mando y Control que sería la encargada de almacenar y distribuir la configuración común, la configuración individual de cada goniómetro, así como la de las misiones asignadas.

Los procesadores goniométricos enviarían los resultados obtenidos a la BBDD Intermedia y a la BBDD Histórica. Esta última recibiría los datos de la misión y los parámetros de configuración asignados a cada goniómetro en el momento de ejecución de la misión, al objeto de poder reproducir con fiabilidad todos los datos iniciales y los resultados obtenidos en cualquier momento temporal.

La BBDD Intermedia sería la encargada de la recogida de los datos obtenidos por cada goniómetro según los parámetros de configuración y las misiones asignadas en curso, de esta forma proporcionarían las interceptaciones obtenidas al interfaz hombre máquina en tiempo útil. Este software utilizará la estadística que proporcione la BBDD Histórica.

Se debe ejecutar en un interfaz hombre máquina que recoja la posibilidad de activar las siguientes alarmas y análisis, utilizando las técnicas anteriormente descritas referentes a MACHINE LEARNING y Detección de Anomalías:

- Alarmas sobre aumento de actividad de las frecuencias asignadas de interés.
- Alarmas sobre la disminución de actividad de las frecuencias asignadas de interés.
- Alarmas sobre la actividad de las frecuencias propias.
- Alarmas sobre cambio de horas habituales de comunicaciones.

#### 4. Conclusiones y líneas futuras

En definitiva, para poder abordar el problema de la exploración **off-line** y detección de alarmas, se debería emplear una arquitectura cliente-servidor flexible [5] que proporcionara un conjunto completo de herramientas para llevar a cabo la vigilancia por radio. Este sistema debería adquirir y describir rápidamente cualquier señal radio, y posteriormente realizar un análisis detallado de señales específicas de interés, tanto en tiempo real como **off-line**. El análisis debería incluir la detección, localización, clasificación y archivo de las actividades radioeléctricas. Cuando se detectase una señal, el sistema determinaría automáticamente la dirección de la fuente de energía y todos los demás parámetros, y presentaría esa información al operador. Esta información se archivaría automáticamente para análisis futuros (**off-line**) o se podría pasar simultáneamente en tiempo real a las estaciones de trabajo del cliente (operador).

Este sistema debería constar de los siguientes subsistemas, figura 3:

- Array de antena de control / DF y distribución de RF.

Para la radiogoniometría, el sistema se debería poder configurar para operar con una variedad de antenas interferómetro.

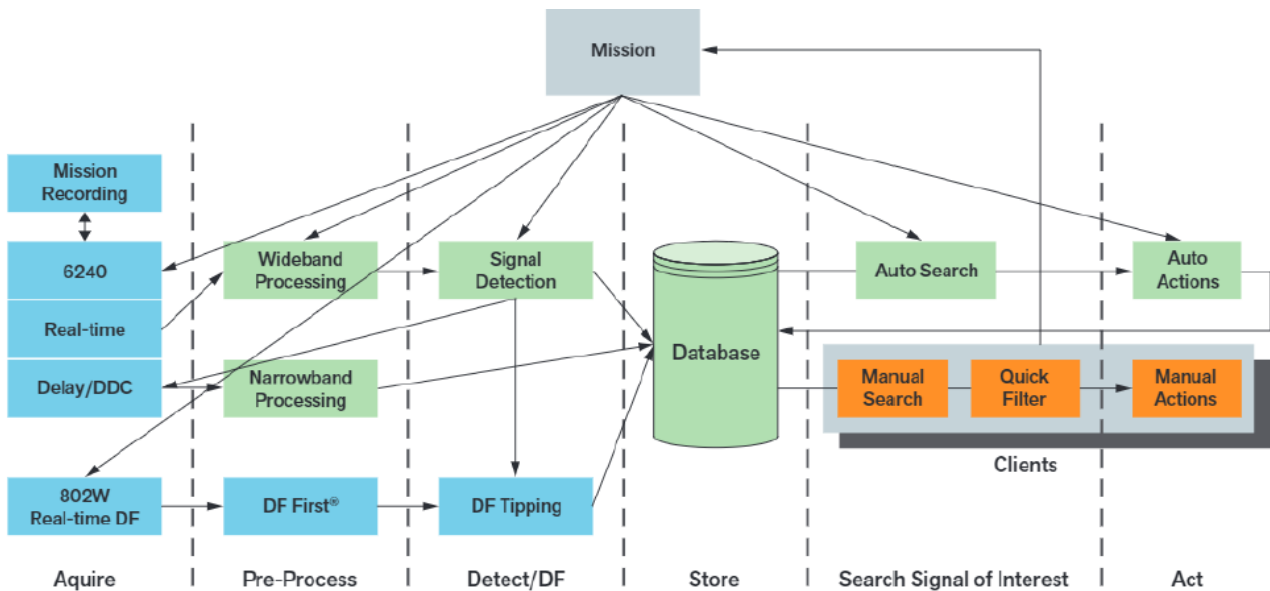
- Adquisición de señal de canal N de banda ancha y procesador DF.

Cada canal constaría de un preselector de banda ancha, un digitalizador de alta velocidad y un procesador de señal digital. Estos procesadores detectarían simultáneamente la actividad de la señal en cada canal y realizarían DF en los canales activos. La actividad espectral y los datos DF se enviarían al controlador para su posterior procesamiento.

- Adquisición y recopilación de señales.

El controlador administraría el acceso de los clientes a los procesadores DF, además registraría los resultados sin procesar (en crudo) para almacenarlos en una base de datos local privada.

- Estaciones de trabajo para tareas del sistema y análisis de señales en tiempo real y **off-line**
- Interfaz de sistema externo y multi-sitio.



**Figura 3.** Esquema de subsistemas (figura tomada de 802W Wideband HF COMINT system)

Este sistema debería integrar una interfaz gráfica de usuario que detectase y catalogase automáticamente todas las señales, para que el operador pueda examinar todas las detecciones o buscar señales específicas de interés utilizando una lista integrada, un espectrograma y mapas. Se debería poder limitar los resultados mostrados a solo señales de interés deseadas, además de poder realizar una búsqueda para encontrar instantáneamente señales similares por frecuencia, huella espectral o geolocalización.

Esta interfaz debería permitir evaluar automáticamente las interceptaciones entrantes según unos criterios de búsqueda. Las interceptaciones que fueran coincidentes deberían desencadenar acciones automatizadas como **alertas** del operador, etiquetado, clasificación de la modulación, grabación en tiempo real, grabación inteligente (grabación basada en criterios de modulación de señal) y geolocalización. Estas tareas de automatización ayudarían a los operadores notificando **alarmas**. Los operadores deberían poder definir áreas de interés para buscar señales por geolocalización.

En relación con líneas futuras, se vislumbran:

- SDR / CR. Aprovechar la flexibilidad que ofrece la radio definida por software (SDR) aplicada a receptores, y más concretamente las radios cognitivas (CR) para mostrar mejores prestaciones en cuanto a reconfiguración de la frecuencia de las antenas y filtrado de ruido[7]. Se propone un enfoque cognitivo, llamado selección de antena cognitiva (CASE), para cambiar secuencialmente los elementos del array de antenas en función de observaciones anteriores.
- Metamateriales. Materiales inteligentes dotados de propiedades electromagnéticas inusuales[8], que se podrían aplicar para fabricación de antenas receptoras utilizando cristales electromagnéticos (antenas de cristal) que permite la eliminación de espúreos en filtros de microondas.
- Receptores fotónicos. Convierten las ondas electromagnéticas en fotones que viajan a la velocidad de la luz. Al procesar la información en fotones en lugar de electrones, se puede extraer y analizar más señales y más rápido[9].

## Referencias

1. Manual del sistema R&S DDF550, wideband direction finder.
2. MATHWORKS machine learning ebook "Introducing machine learning", 2016
3. Radiomonitoring & radiolocation, catalog 2016, de Rohde & Schwarz
4. Monografías del SOPT. La guerra electrónica en España, octubre 2009
5. Ficha de características técnicas del 802W Wideband HF COMINT system, 2016
6. Documentación del II Curso de Analista de Información Electrónica del E.T.
7. [https://www.researchgate.net/publication/224263423\\_On\\_antennas\\_for\\_Cognitive\\_Radios](https://www.researchgate.net/publication/224263423_On_antennas_for_Cognitive_Radios)
8. [www.mundodigital.net/metamateriales-los-materiales-inteligentes/](http://www.mundodigital.net/metamateriales-los-materiales-inteligentes/)
9. <https://www.dasphotonics.com/defense/>