LoRaWAN – Parte 6
DESCUBRIMIENTO DE LORA -SDR TDT

Ya como complemento a esta unidad veremos un método relativamente sencillo de poder descubrir y escanear nodos LoRa en nuestro alrededor, esto nos será útil en caso de tener que auditar la seguridad de una red que controlemos o para comprobar y testear el correcto funcionamiento de nuestra propia red.

Antes de nada, es necesario decir que estas pruebas están realizadas únicamente utilizando LoRa como método de transmisión, es decir no se trata de una red LoRaWAN sino de un único emisor emitiendo el mensaje “Hello, world!”, es importante remarcar esto ya que en el caso de LoRaWAN deberíamos poder evadir las capas de seguridad adicionales que se implementan y que hemos visto anteriormente.

Para realizar las pruebas simplemente necesitaremos un decodificador TDT Usb, eso sí necesitaremos uno con el Chipset RTL2832U, esto es debido a su amplio rango de frecuencias como receptor que nos permite funcionar entre los 50MHz y los 2200MHz y además es compatible con gran cantidad de programas SDR (Software Defined Radio), los cuales nos van a permitir trabajar con las tramas y paquetes recibidos a través de este receptor TDT de bajo coste (Alrededor de 8€)

Ilustración 1 - Receptor TDT con soporte RTL-SDR

Las frecuencias que abarca nos permiten recibir una gran cantidad de tecnologías en ese rango como podemos observar, en el siguiente gráfico:

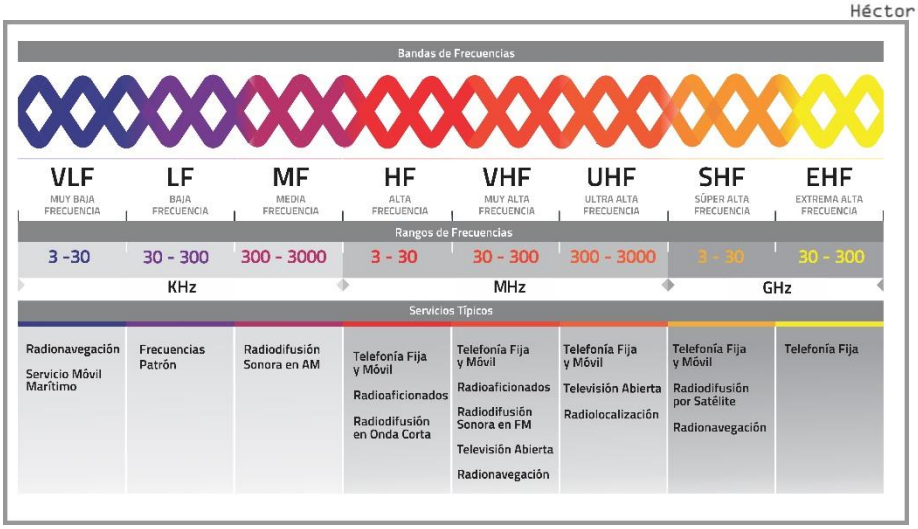

Ilustración 2 - Tabla de frecuencias y usos

Como podemos ver, también tendremos disponibles para la escucha las frecuencias correspondientes a la tecnología LoRa que se encuentran dentro del rango UHF.

Antes de comenzar deberemos instalar algún software SDR en nuestro equipo, se recomienda el uso de GNURadio Companion ya que existe una gran cantidad de documentación al respecto de cómo instalarlo y como hacer funcionar nuestro receptor TDT en el, lo cual nos facilitará mucho el arranque dentro de este mundo.

Con nuestro software instalado y funcionando deberemos cargarle una serie de módulos o bloques que nos van a permitir trabajar con paquetes LoRa dentro de nuestro programa para ello haremos uso del software desarrollado por Bastille Threat Research Team (https://www.bastille.net/) disponible en si Github, instalándolo tal y como nos indican en sus instrucciones mediante los siguientes comandos:

```
git clone git://github.com/BastilleResearch/gr-lora.git

cd gr-lora

mkdir build

cd build

cmake ../

make

sudo make install

sudo ldconfig
```

Una vez instalados los nuevos módulos de GNURadio Companion abriremos el framework para comenzar a definir nuestro programa, dejando los bloques que vemos a continuación:

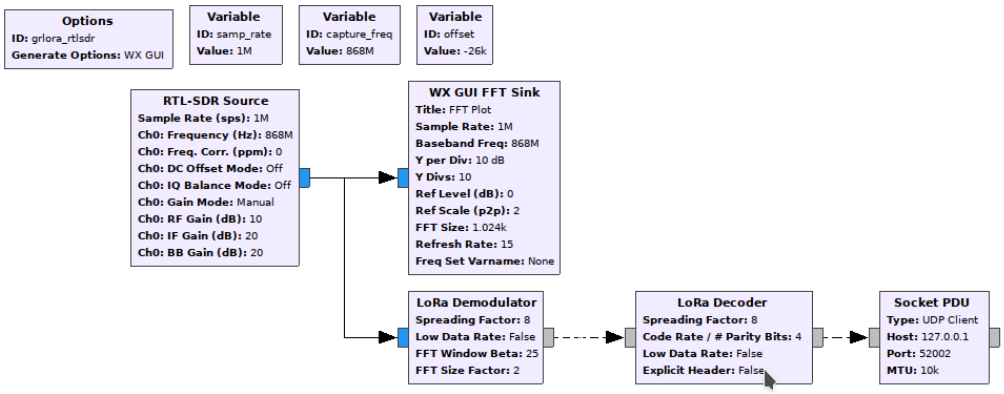

Ilustración 3 - Programa en GNU Radio

Se trata de un método de programación visual que nos facilita ciertas tareas, vemos como existen bloques de variables que luego podemos reutilizar en otros bloques pro ejemplo y bloques para tareas específicas como son los bloques de LoRa.

También definimos un bloque RTL-SDR Source para indicar a nuestro programa que debe leer los datos que se reciban en nuestro receptor TDT, dentro de la frecuencia 868MHz, posteriormente esa información se envía a un bloque que nos mostrará una gráfica sobre la señal recibida centrándose también como vemos en la banda de 868MHz.

La salida de nuestro TDT además es enviada a los módulos LoRa que se encargan de emular y decodificar el contenido del paquete y pasarlo a un socket UDP que podremos leer posteriormente para comprobar la información recibida.

Podríamos de esta manera enviar esa información a otro servidor donde la procesemos o incluso a un fichero que pudiéramos analizar más tarde en profundidad.

Una vez que ejecutamos nuestro programa veremos que nos aparece una nueva ventana con la gráfica de estado de la banda 868MHz y que al arrancar nuestro emisor LoRa se recibe una variación de señal que nos indica que en esa banda está habiendo emisiones.

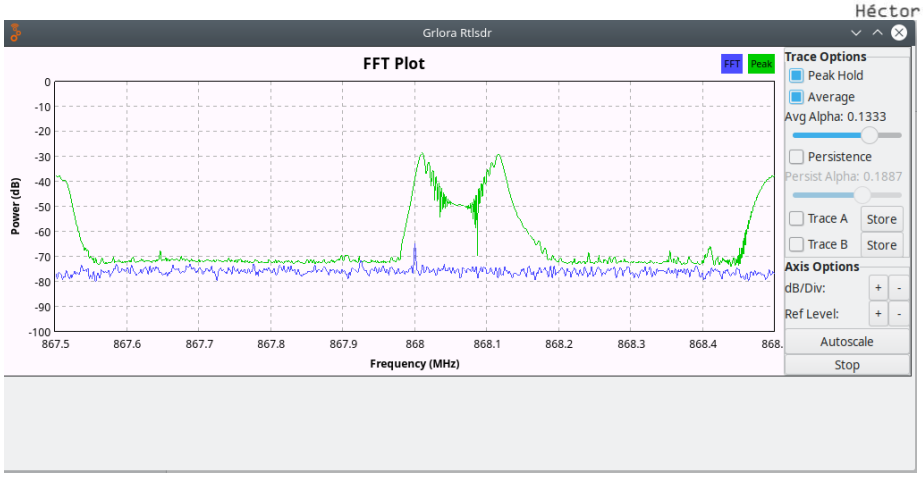

Ilustración 4 - Onda capturada

Como hemos dicho hemos enviado además esa información también a un socket UDP para poderla recibir y leer haciendo uso del comando netcat poniéndolo a la escucha en ese mismo puerto y viendo el mensaje enviado.

```
root@hector6598-laptop:~/gr-lora2/build# nc -l -u 127.0.0.1 52002
Hello, world!
```

Ilustración 5 - Mensaje en claro

Estas pruebas nos muestran la importancia de implementar siempre medidas de seguridad dentro de las comunicaciones inalámbricas ya que como podemos ver son fácilmente accesibles al expandirse en un rango muy amplio.