



UNIVERSIDAD DE GRANADA

Fundamentos de Redes

LoRa y LoRaWAN

Juan Ocaña Valenzuela
Guillermo Sandoval Schmidt

21 de noviembre de 2018

Versión: 1.0

Índice

1. LoRa	3
1.1. Qué es y cómo funciona	3
1.2. Ventajas y principales usos	3
1.3. LoRa vs. SigFox	4
2. LoRaWAN	4
2.1. Qué es LoRaWAN	4
2.2. Clases de dispositivos	5
2.3. Activación y seguridad	6
3. Conclusiones	7
4. Bibliografía	8

1. LoRa

1.1. Qué es y cómo funciona

LoRa (de Long-Range) es una tecnología inalámbrica de comunicación, como pueden ser WiFi o Bluetooth, que funciona en un rango amplio (como su nombre indica) y está basada en radio, como AM o FM.

Desarrollada originalmente por la empresa *Semtech*, aunque actualmente administrada por *LoRa Alliance*, la tecnología LoRa está basada en la técnica de **modulación chirp**. La empresa la define como «*el ADN del IoT*».

En Europa utiliza las frecuencias 433 MHz y 868 MHz.

Modulación chirp

La modulación chirp es una técnica de modulación por pulsos basada en el espectro ensanchado. Esta última se emplea para la transmisión de datos digitales por radiofrecuencia.

Su fundamento básico es la transmisión a lo largo de una banda muy ancha de frecuencias, mayor que el mínimo necesario para la transmisión que deseamos realizar. Esto puede parecer un desperdicio de recursos; sin embargo, al combinarlo con sistemas que utilizan la frecuencia, maximiza su rendimiento.

Este tipo de señal, una vez ensanchada, puede coexistir con otras señales en banda estrecha, aportando únicamente un ligero ruido.

1.2. Ventajas y principales usos

- Se ve poco afectada por las interferencias
- Tiene poco consumo
- Como su nombre indica, permite comunicaciones a largo alcance
- Realiza conexión punto a punto

Estas características lo hacen excelente para su uso en redes de IoT en las que los sensores utilizados no tienen por qué disponer de corriente eléctrica.

Algunos de sus usos podrían ser aplicaciones para *Smart Cities*, aplicaciones en lugares con poca cobertura, para construir una red privada con sensores y actuadores, o para monitorizar datos médicos y datos medioambientales.

1.3. LoRa vs. SigFox

SigFox es otra tecnología inalámbrica centrada en IoT. A continuación, presentamos las diferencias y similitudes entre LoRa y SigFox.

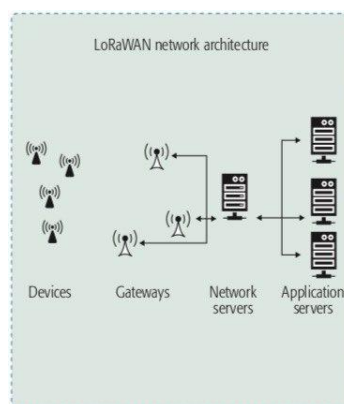
- Ambas utilizan señales de gran alcance.
- Ambas requieren poca energía.
- Para usar SigFox, además de comprar el módulo correspondiente, hay que contratar un plan de suscripción.
- LoRa puede operar de forma bidireccional, mientras que SigFox solo de manera unidireccional.
- La API de SigFox es más simple pero menos configurable. La API de LoRa es de bajo nivel, por lo que, a pesar de que su integración sea más compleja, nos permite configurarla a nuestro gusto.
- Ambas tecnologías ofrecen funciones de seguridad, ya que tienen comunicación cifrada. Sin embargo, ninguna de ellas ofrece comunicaciones encriptadas.

2. LoRaWAN

2.1. Qué es LoRaWAN

LoRaWAN es una especificación de redes LPWAN (Low Power Wide Area Network). Esta se encarga de unir los diferentes dispositivos LoRa, encargados de gestionar los parámetros de la conexión.

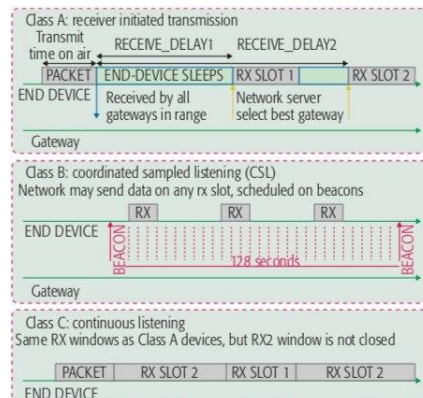
Siguiendo la estructura del Modelo OSI, la tecnología LoRa (de la que ya hemos hablado) formaría el nivel 1 y LoRaWAN formaría el nivel 2. LoRaWAN cuenta con una arquitectura en forma de estrella, que significa que nuestros dispositivos están todos conectados a un punto central por el que deben pasar todas las comunicaciones.



Esquema de red LoRa

2.2. Clases de dispositivos

LoRaWAN permite la comunicación bidireccional, aunque sea asimétrica, ya que las transmisiones hacia arriba se ven claramente favorecidas. Debido a esto, podemos diferenciar 3 tipos de dispositivos, que enumeraremos como de clase A, B y C, cada uno con sus ventajas e inconvenientes.



Representación de las clases de dispositivos

Clase A

Los dispositivos de Clase A se encargan de enviar información únicamente, aunque pueden escuchar, pero de forma muy limitada (únicamente después de enviar datos a la red). Esto los hace óptimos para aplicaciones de monitorización, pues sólo envían información, y consumen poca energía. La duración de las baterías es muy elevada.

Clase B

Esta clase de dispositivos presentan una escucha por muestreo, lo que se conoce como *Coordinated Sample Listening (CSL)*. La red envía señales baliza de forma periódica, y cuando el dispositivo las recibe, comienza a escuchar durante un tiempo determinado en distintas ventanas de recepción hasta que llegue la siguiente baliza. Esto incrementa el gasto energético del dispositivo. El modelo suele aplicarse a actuadores con baterías.

Clase C

Por último, los dispositivos de Clase C escuchan durante todo el tiempo, y tienen un gasto energético mayor. Suelen ser actuadores que requieren corriente.

2.3. Activación y seguridad

La especificación de LoRaWAN dispone de una serie de identificadores para dispositivos, aplicaciones y *gateways* (pasarelas), por ejemplo:

- **DevEUI:** identificador del dispositivo (64 bits - único)
- **DevAddr:** dirección del dispositivo (32 bits - no único)
- **AppEUI:** identificador de aplicación (64 bits - único)
- **GatewayEUI:** identificador de gateway (64 bits - único)

Los dispositivos LoRaWAN disponen de un **DevEUI** asignado por el fabricante. Sin embargo, las comunicaciones se realizan utilizando el **DevAddr**.

Activación

Al activar un dispositivo, formará parte de la red LoRaWAN y se comunicará con los diferentes servidores de aplicación.

Los dispositivos pueden ser activados de dos formas:

Over The Air Activation (OTAA)

Cuando un dispositivo se activa mediante OTAA, deriva las claves de sesión durante la operación de unión. Tanto la petición de unión como los mensajes de aceptación incluyen un código de integridad de mensaje (MIC) cifrado según la *AppKey*. Así, un extremo puede verificar que el otro conoce su clave y autenticarlo de esta forma.

Activation By Personalization (ABP)

La activación por personalización consiste en introducir manualmente la información en ambos dispositivos (*hardcoded*).

Independientemente del método de activación del dispositivo, se utilizan los siguientes campos:

- DevAddr
- AppEUI
- **NwkSkey:** clave de sesión de red
- **AppSkey:** clave de sesión de aplicación

Propiedades

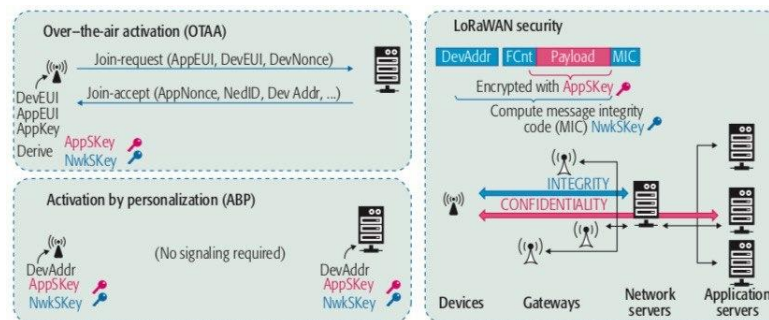
Las principales propiedades que cumple la seguridad de LoRaWAN son **autenticación mutua, integridad y confidencialidad**.

La integridad se logra gracias a un código MIC, que es usado tanto por el dispositivo como el servidor de red.

La confidencialidad se logra ya que el tráfico de datos no solo se encripta en la interfaz over-the-air, si no que se transmite de manera segura por el núcleo del operador de red.

El esquema de encriptado está basado en AES, lo que permite la encriptación entre el dispositivo y el servidor de red.

Estas características nos evitan tener que implementar otras capas de seguridad, permitiendo mantener un gasto de energía, una complejidad y un coste relativamente bajo.



Esquema de la seguridad en LoRaWAN

3. Conclusiones

LoRaWAN es una tecnología centrada en el ahorro de energía, ya que, a pesar de sus limitaciones, lo compensa con un gasto energético mínimo y un rango amplio, lo cual es idóneo para montajes de IoT que, por ejemplo, requieran monitorización de algún parámetro natural.

También cabe destacar que LoRa se ve afectado en espacios cerrados, pues la señal pierde mucha potencia al atravesar paredes y suelos. Por tanto, no es recomendable utilizarlo en, por ejemplo, un aparcamiento.

En conclusión, LoRa es una tecnología barata de implementar y utilizar, y el estándar LoRaWAN permite su aplicación en el cada vez más amplio campo del *Internet de las Cosas*.

4. Bibliografía

<http://lorawan.es/>
<https://lora-alliance.org/about-lorawan>
<http://www.alfaiot.com/index.php/es/2018/05/26/que-es-lora/>
https://es.wikipedia.org/wiki/Espectro_ensanchado
<https://www.thethingsnetwork.org/docs/lorawan/address-space.html>
<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8291115&tag=1>

Agradecimientos especiales a Jorge Navarro Ortiz, profesor del Departamento de Teoría de la Señal, Telemática y Comunicaciones, por sus consejos; y a José Baena Cobos, por la cesión de un módulo RTL-SDR para realizar pruebas.