## LoRaWAN – Parte 4
## VELOCIDAD DE TRANSMISION

Como hemos indicado al inicio de estos artículos las redes LoRaWAN no destacan por su alta velocidad de transmisión de datos, por lo que es importante conocer las limitaciones que afectan a este campo a la hora de decidir si este tipo de redes pueden sernos útiles en un determinado proyecto.

Una de las limitaciones que debemos tener en cuenta no es técnica sino normativa, ya que el Instituto Europeo de Normas de Telecomunicaciones (ETSI) dictamina que existe una limitación en el tiempo de uso de la red limitado al 1% para los nodos y en un 10% para los Gateways.

De esta manera debemos saber que si enviar una trama nos ocupa 100ms deberemos estar 9900ms sin transmitir información a la red. Pero esto no es tan sencillo ya que tenemos otro factor a tener en cuenta en esta ecuación y es el Spread Factor (SF) o en español el factor de esparcimiento.

El factor de esparcimiento nos permite enviar mensajes de una manera más lenta, pero alcanzando una mayor distancia, pero aquí es donde encontramos el problema, cuanto más lento emitamos menos paquetes podremos transmitir al tener que cumplir la regla del 1%.

Con esta información ya podemos darnos cuenta de que para conocer la velocidad efectiva que podremos tener en nuestros nodos será necesario conocer la distancia a la que estarán de un Gateway para poder conocer su SF y de esta manera poder calcular el tiempo que podrá emitir y la cantidad de datos que transmitirá para poder conocer la velocidad final de transmisión.

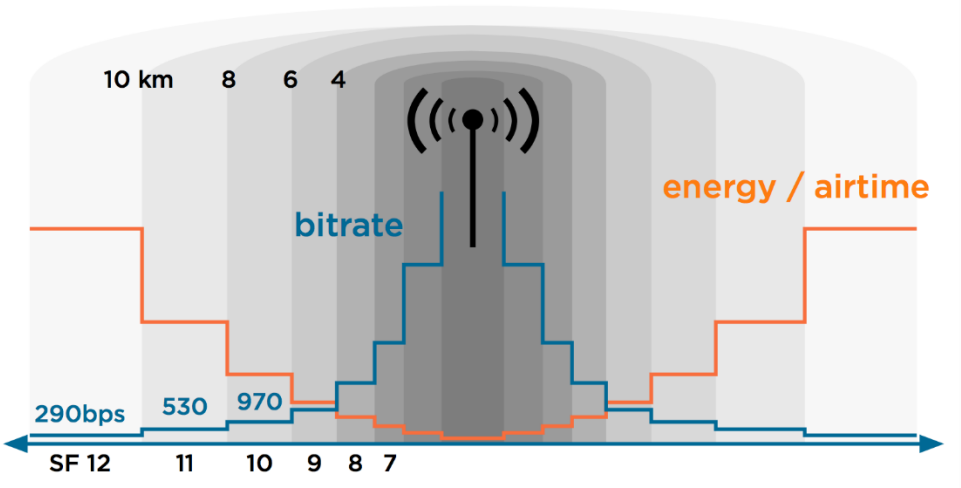


*Ilustración 1 - Espectro alcanzado por LoRa*

Para poder calcular estos datos lo mejor es apoyarse en el uso de calculadoras on-line para estos parámetros LoRa o incluso usar herramientas como la desarrollada por el usuario de Github tampoco https://github.com/tanupoo/lorawan_toa que nos permitirá desde una herramienta Python realizar estos cálculos de una manera sencilla.

Por esto es que la velocidad de las redes LoRa puede variar entre los 250bps hasta los 50kbps.

En este punto es interesante hacer hincapié en un dato que hace más interesante aún a la tecnología LoRa y es que estamos diciendo que mismos nodos de una misma red pueden funcionar a velocidades diferentes, es más un mismo nodo puede variar su SF dependiendo de la distancia que tenga hasta el Gateway más cercano, por ello veremos que para poder establecer una comunicación entre varios dispositivos deberemos sincronizar todas estas velocidades.

Esta tarea es llevada a cabo por los servidores IoT de LoRaWAN usando para ello el mecanismo ADR ya nombrado anteriormente de manera que usando la información contenida en el Frame Header se analicen los contadores de paquetes y los datos SNR (Signal-to-noise) para conocer las velocidades y ganancias de los paquetes transmitidos y de esa manera poder configurar el bit ADR de las tramas LoRa que servirá a los servidores para poder adaptar las comunicaciones entre los diferentes nodos.

A continuación, se deja un diagrama de flujo en el que se puede ver el proceso de configuración de ese bit ADR.

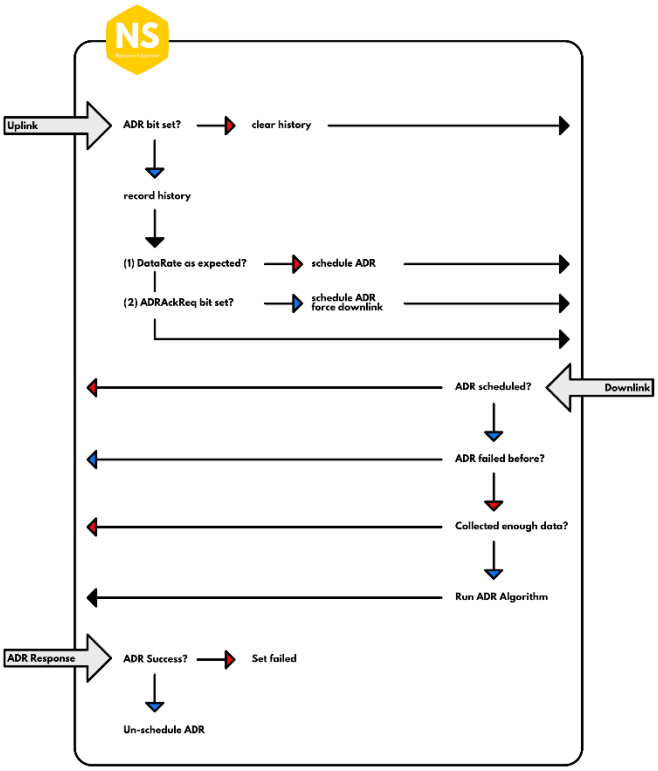


*Ilustración 2 - Proceso de grabado del bit ADR*

## SEGURIDAD

Tal y como hemos comentado ya la seguridad es un factor imprescindible dentro de las redes IoT ya que en muchos entornos estas redes transportan datos críticos de salud y de control de infraestructuras que pueden provocar un grave problema en caso de no estar correctamente gestionados.

LoRaWAN está basada en el estándar IEEE 802.15.4 implementa dos capas adicionales de seguridad, a nivel de red y a nivel de aplicación, como hemos podido ver en el detalle de las tramas enviadas por los dispositivos.

La capa de red con el uso de la Network SKey es capaz de generar el MIC que nos aporta seguridad en cuanto a la integridad del mensaje y su procedencia, mientras que la APP SKey es la encargada de cifrar la información que va a ser transmitida, este cifrado se realiza utilizando el algoritmo AES 128.

Ahora bien, ¿Cómo generamos estas claves y las almacenamos en los nodos finales? Pues tenemos dos tipos diferentes de autenticación posibles para poder dar acceso a nuestros nodos a la red.

- **ABP:** Activación por personalización o Activación By Personalisation, este método consiste en almacenar directamente la NwSKey y la APPSKey en la memoria de nuestro nodo en el mismo momento en el que este es fabricado, de esta manera el dispositivo al ponerse en marcha ya estaría pre registrado en la red.

  El problema de este método es claro, si en algún momento variamos estas claves porque se hayan visto comprometidas, deberemos volver a grabar estas nuevas claves en todos y cada uno de los dispositivos de nuestra red con el esfuerzo que esto supone.

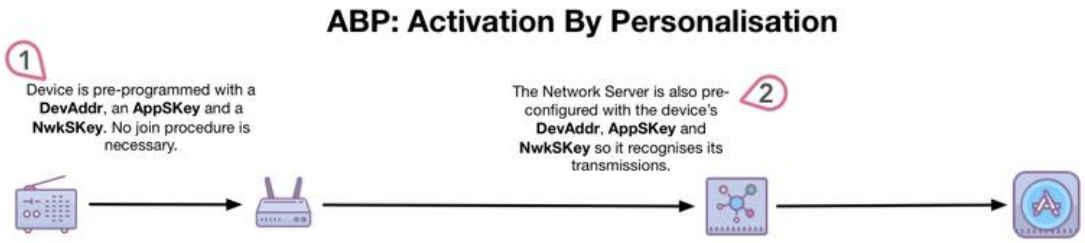


*Ilustración 3 - Autenticación ABP*

Este tipo de autenticación está pensado en entornos con pocos nodos y que además estén accesibles para poder realizar estos cambios de claves si fuera necesario, además veremos que es un protocolo algo más débil por lo que no es recomendado para entornos en los que enviemos datos críticos.

- **OTAA:** Activación al vuelo o Over-The-Air Activation, este método es más avanzado y se basa en el envío de una solicitud de unión a la red enviada por el nodo hacia el Gateway, y este basándose en el DevEUI el AppEUI y el AppKey mandará un paquete de confirmación y posteriormente un paquete con el NwkSKey y el APPSKey para que sean almacenados dentro de la memoria del nodo.

  Este mecanismo nos aporta un plus de seguridad ya que en caso de necesitar hacer algún cambio en las NwSKEY y las APPSKey los nodos simplemente volverán a enviar una solicitud de unión a la red y les serán enviadas las nuevas claves.

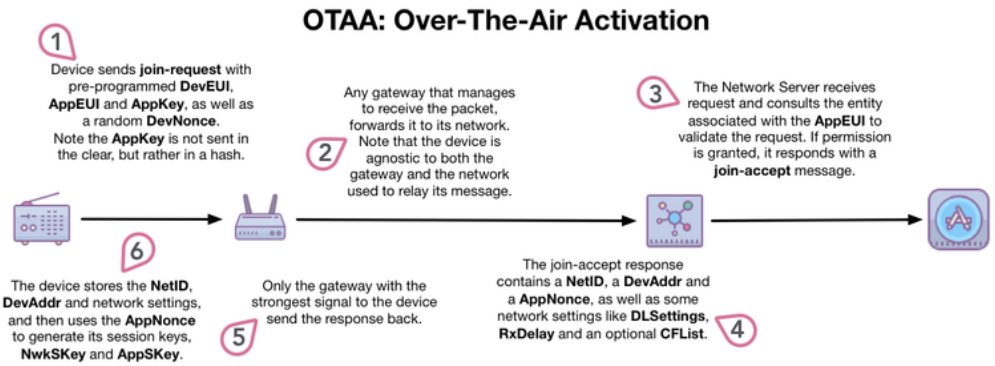


*Ilustración 4- Autenticación OTAA*

Como podemos observar este método es bastante más seguro, pero por el contrario genera más tráfico al necesitar ciertos paquetes más para poder realizar el proceso de unión a la red.

Lo normal es usar este método en redes más extensas o con nodos remotos a los que no tenemos acceso de manera habitual.

Dentro de la tecnología LoRaWAN es necesario tener en cuenta también la seguridad de los servidores IoT que utilicemos y cerciorarnos de usar las herramientas de seguridad que nos aporta el protocolo TCP/IP como puede ser el uso de servicios VPN y la securización del tráfico mediante HTTPS.

Una vez que tenemos una idea general del funcionamiento de la red LoRaWAN es interesante conocer los posibles ataques que puede sufrir nuestra red para tratar de mitigarlos:

- **Replay Attacks:** Este tipo de ataques se basan en la captura y guardado de los paquetes íntegros de la comunicación LoRa, mientras se analiza la red de manera paralela centrándose sobre todo en los contadores de los paquetes.

  Como hemos visto estos contadores son muy importantes ya que nos ayudan a descartar paquetes que estén duplicados en la red y a ordenar las comunicaciones, de manera que, si un paquete tiene por ejemplo el valor de contador 6 y la red está gestionando ya el paquete 10, aunque lo reenviemos a los nodos será descartado al ser menor al actual.

  Pero existe un problema y es que los contadores debido a la estructura de las tramas LoRa tiene un límite y deben ser reiniciados cada cierto tiempo, momento en el cual un atacante puede aprovechar para enviar el paquete capturado y que sea aceptado por la red.

Para ver la repercusión de este ataque vamos a imaginar que se usa para lanzar una alerta por ejemplo de incendio, un atacante podría capturar los paquetes que indican que todo va bien y dedicarse a reenviarlos en el momento que corresponda para indicar al sistema que todo es correcto a pesar de que pueda haber un incendio en esos momentos.

Este tipo de ataques afecta especialmente a los nodos autenticados mediante el método ABP ya que sus paquetes no cambian nunca al usar siempre las mismas APPSKey y NwSKey por lo que una solución puede ser el uso de sistemas OTAA siempre que sea posible.

- **Jamming Attacks:** Este tipo de ataques buscan más que un robo de información simplemente una denegación de servicio de la red, ya sea simplemente para parar un servicio o como complemento de otros ataques que se puedan tratar de realizar.

  Consiste básicamente en el envío de una gran cantidad de señales de mayor potencia que las señales reales de nuestra red de manera que se sature el espectro radioeléctrico provocando interferencias que puedan hacer que los nodos no se puedan comunicar con los Gateway o viceversa.

  En el caso de LoRa este ataque tiene algo más de dificultad ya que una de las características que tiene la modulación de espectro ensanchado de la que hace uso LoRa es que es más estable y lo hace más resistente a este tipo de ataques, aunque en distancias largas es donde podemos tener una mayor posibilidad de sufrirlo.

  No hay una mitigación posible de este tipo de ataques, más que el uso de una mayor cantidad de Gateways y la calidad de estos para tratar de tener el máximo de potencia permitida disponible, haciendo más complicado que nos afecte el ruido generado

- **Eavesdropping Attack:** Este ataque está orientado a tratar de obtener acceso a la red basándonos en que se hayan utilizado claves débiles para el proceso de autenticación de los nodos.

  El objetivo de este ataque es recoger paquetes con la finalidad de conocer su payload ya que podemos saber que el resultado cifrado de ese payload para un paquete con un determinado contador y payload si siempre usa la misma clave será idéntico de manera que podremos generar diferentes paquetes variando las

claves hasta obtener el mismo resultado, momento en el cual podremos configurar ciertos nodos maliciosos que se unan a la red con claves válidas.

Se trata de un ataque que hace uso de una gran cantidad de cómputo para poder generar diferentes claves y la comprobación de paquetes, pero si durante el despliegue de nuestros nodos elegimos una clave débil por ejemplo 112233445566778899AABBCCDDEEFF o claves que puedan estar disponibles por otros medios estas pruebas se reducen significativamente poniendo en riesgo la seguridad de la red.

Este tipo de ataques es fácilmente mitigable si desde el diseño de nuestra red ya tenemos en cuenta que debemos generar claves robustas de manera pseudoaleatoria, y por su puesto usando OTAA en vez de ABP podremos cambiar más a menudo nuestras claves haciendo que sea más complicado obtenerlas mediante este tipo de vulnerabilidad.

- **Wormhole Attack:** Como dijimos anteriormente los ataques de jamming a las redes muchas veces ocultan otras intenciones, y veremos como este tipo de ataque se aprovecha de esa vulnerabilidad en combinación con un ataque de Replay de paquetes.

  La mecánica del ataque es sencilla, debemos estar controlando la red y realizar una captura de un paquete, lo ideal es poder capturar un paquete de confirmación acceso a la red de manera que lo almacenemos y en ese mismo instante comenzaremos un ataque jamming contra el nodo para tratar de bloquear sus paquetes legítimos. En ese momento reenviaremos el paquete capturado con la intentción de que el Gateway lo acepte y nos podamos unir a la red de manera normal y enviar datos dentro de la misma siendo un nodo externo a la red legítima.

  La mitigación de este tipo de ataques es compleja ya que debemos controlar dos factores diferentes, pero la lógica nos dice que lo más recomendable es poder evitar alguno de los dos ataques usando los métodos que hemos visto en cada uno de sus apartados o combinándolos entre sí.

- **Tampering de dispositivos:** En español sería un ataque de manipulación, como su nombre indica consiste en manipular el dispositivo con la intención de encontrar algún puerto o sistema al descubierto que nos permita acceder directamente a la memoria del dispositivo para poder extraer las claves.

Este tipo de ataque requiere de conocimientos avanzados de electrónica ya que consiste en atacar directamente al hardware de nuestros nodos por lo que en muchas ocasiones necesitaremos poder localizar y extraer componentes del nodo que queramos atacar para poder realizar esa extracción de datos.
La mitigación de este tipo de ataques se realiza desde el diseño de los dispositivos tanto electrónicamente como en sus carcasas añadiendo por ejemplo resinas que dificulten el acceso a la electrónica y no dejando puertos de debug o de desarrollo al alcance de cualquiera.

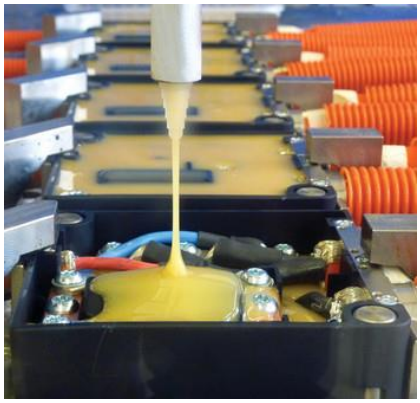

*Ilustración 5 - Ejemplo de potting anti-tamper*

Por supuesto que otro método de protección es el almacenar las claves de cifrado dentro de áreas seguras y cifradas de la memoria o el uso de chips de cifrado para esta tarea, añadiendo así otra nueva capa de protección a los elementos de nuestra red.

- **Otros ataques físicos:** Además del ataque de tampering, es muy importante tener en cuenta que por las características de las redes LoRa es muy posible que tengamos nodos que puedan encontrarse más aislados siendo muy sencillo el ataque de los mismos a nivel de servicio o de actos vandálicos, es por esto que es muy importante realizar estudios de cobertura que nos ayuden a conocer el rango de acción de nuestra red, y dentro de esos rangos buscar localizaciones que aporten una mayor seguridad a nuestros nodos y Gateways, como puede ser sitios elevados o de difícil acceso.

  Además, es importante tener en cuenta que a pesar del bajo consumo eléctrico de los nodos puede ser interesante contar con fuentes redundantes de energía que nos protejan de una perdida de servicio producida por un corte eléctrico ya sea accidental o provocado.