Estudio de la arquitectura y el nivel de desarrollo de la red LoRaWAN y de los dispositivos LoRa.

Ignacio Ordóñez Monfort

Resumen

Se define el Internet de las Cosas (IoT en inglés) como la conexión de todo tipo de objetos a la red Internet. Dicha conexión convierte al objeto en un elemento que participa de forma activa en el flujo de información en Internet. La plena conectividad abre un nuevo mundo de posibilidades que supone una verdadera revolución y evolución de la red Internet. La viabilidad del IoT pasa por el desarrollo tecnológico de nuevos dispositivos y de nuevas redes que posibiliten la conexión global de objetos. En el presente artículo se realiza un estudio sobre las diversas definiciones del IoT que se concreta en una serie de requisitos esenciales del IoT y las características de las redes de conexión sobre las que sustentarlo. Se realiza posteriormente un estudio en profundidad de las características de LoRA/LoRaWAN que puedan limitar o favorecer su uso como red de implementación del IoT valorando de forma individualizada cada una de ellas. Finalmente se realiza un análisis sobre el nivel de desarrollo, madurez y disponibilidad de productos LoRaWAN en el mercado.

I. IoT Y REDES LPWAN.

Se ha establecido el término Internet de las Cosas, en adelante IoT, para definir la conexión de todo tipo de objetos a la red Internet, desde objetos simples de uso cotidiano a objetos complejos. Son enormes las posibilidades que ofrece la conexión de todo tipo de objetos a Internet: multitud de nuevas aplicaciones y servicios, explotación de Internet en nuevos ámbitos,… De aquí que la idea del IoT ha ido cogiendo fuerza en los últimos años.

De acuerdo con lo establecido en [13]: Los objetos, por el hecho de estar conectados, sufren una especie de "metamorfosis" que los convierte en elementos que interactúan a un nivel superior con el mundo que los rodea. Esta interacción se realiza mediante el intercambio de información entre dispositivos como consecuencia de algún cambio o evento en el entono físico del objeto. De esta forma, los objetos pasan a tener un papel activo en el mundo real con la capacidad de responder frente a un evento desencadenando algún tipo de acción. Los objetos pasan por lo tanto a ser participantes activos en los procesos sociales, de negocios, de información,... lo que lleva asociado no sólo cambios de tipo tecnológico sino industriales, organizativos y psicosociales.

En la actualidad no están definidos de forma rigurosa los requisitos que deben cumplir los dispositivos y las redes de comunicación para la implementación del IoT, aunque sí se puede definir aquellos que son esenciales, en concreto:

- Dispositivos de bajo consumo de energía. Los dispositivos de conexión se deben diseñar para que sean energéticamente muy eficientes de forma que puedan operar mediante baterías y que la autonomía de las mismas sea, al menos, de varios años.
- Dispositivos de reducido tamaño. Los dispositivos de conexión deben tener un tamaño adecuado para ser utilizables en cualquier tipo de objeto.
- Movilidad en las comunicaciones. Los dispositivos de conexión y las redes de comunicación deben ser diseñados para asegurar la movilidad total.
- Servicios de localización. Las redes de soporte al IoT deben contar con sistemas de localización de los dispositivos, aspecto fundamental para muchas aplicaciones industriales, de negocio y domésticas.
- Comunicaciones seguras. Se debe asegurar la confidencialidad e integridad de los datos transmitidos. La trasmisión de datos de salud o datos críticos en procesos industriales, por citar unos ejemplos, evidencia de forma clara la necesidad de mantener la privacidad y la integridad de los datos transmitidos.
- Redes de conexión de amplio alcance (varios kilómetros) que acepten un elevadísimo número de dispositivos (cientos de miles). Además deben ser sencillas de implementar y administrar, fiables y robustas.
- Bajo coste de producción de los dispositivos finales así como de los elementos de red.

Según [4] las actuales redes de comunicación inalámbricas de tipo WAN –GSM, UMTS, WIFI,…- no se ajustan de manera adecuada a los requisitos esenciales del IoT por diversos motivos: alcance de la conexiones, coste de los dispositivos e imposibilidad de proporcionar conexión a un elevadísimo número de dispositivos finales. Tampoco son adecuadas las redes locales de bajo consumo por su corto alcance (menos de 1 km). Si bien esto último es subsanable utilizando topologías de tipo *mesh*[2], lo cierto es que la obligada retrasmisión de tráfico proveniente de otros dispositivos eleva el consumo eléctrico de los dispositivos llegando a limitar el tiempo de vida de la batería a no más de un año[6].

Por los motivos expuestos con anterioridad, sólo con el desarrollo de nuevas redes de conexión se puede dar solución tecnológica al IoT. Estos nuevos desarrollos se denominan *Low-Power Wide Area Network* (LPWAN).

En la actualidad hay múltiples propuestas de redes LPWAN, casi todas ellas presentan características comunes[6]:

- Operar en la banda libre ISM por debajo de 1Ghz. Este tipo de señales presentan un menor factor de atenuación al atravesar obstáculos respecto a la banda libre ISM de 2,4 Ghz.
- Poseer esquemas de modulación que posibilitan la creación de enlaces de varios kilómetros en zonas urbanas y de decenas de kilómetros en zonas rurales con muy bajo coste energético. Son dos las técnicas de modulación que principalmente se utilizan:
    - Modulación en banda estrecha y ultra estrecha. Se trata de codificar una señal en una banda cercana a la más estrecha posible o en la más estrecha posible que permita su codificación. La característica principal de este tipo de modulación es que el nivel de ruido para cada canal es muy pequeño lo que permite aumentar el alcance de la señal, como contrapartida la velocidad de transmisión decrece. La decodificación de la señal por parte del receptor es sencilla.
    - Modulación *Spread Spectrum*. Esta técnica de modulación consiste en ensanchar una señal de forma que el ancho de banda de la señal a transmitir sea mucho mayor que el ancho de banda necesario para transmitir la señal inicial. La señal finalmente trasmitida es más robusta frente a interferencias externas por lo que las señales son difícilmente interceptables. Sin embargo, el procesamiento extra al que se somete a la señal a trasmitir hace que los transceptores empleados para la decodificación de la señal sean muy complejos y por lo tanto más costosos.

Si bien hay varias redes o propuestas de redes LPWAN que cumplen los requisitos iniciales para el IoT[8], sólo son tres las que en la actualidad tienen soluciones completas en el mercado: SigFox[16], Ingenu[17] y LoRa[14]. Estas tres redes disponen ya de grandes instalaciones que conectan multitud de dispositivos a Internet. No obstante existe una clara diferencia entre el modelo de negocio seguido por SigFox e Ingenu frente al seguido por LoRa. Tanto SigFox como Ingenu siguen un modelo de negocio totalmente propietario en el que dichas empresas ofrecen todos los servicios del IoT: venta de dispositivos, red de conexión y servicios. En el caso de la red LoRA, la empresa propietaria –Semtech- lo es sólo de la capa física, la capa de acceso al medio se desarrolla de forma abierta por una entidad sin ánimo de lucro denominada *LoRa Alliance*. Semtech sólo comercializa dispositivos. Esto hace que cualquier empresa de TI pueda utilizar esta tecnología para poner en marcha su propia red LPWAN y así ofrecer servicios e infraestructura de red a sus clientes. La red LoRa representa una solución mucho más atractiva desde un punto de vista de negocio que SigFox e Ingenu, es por este motivo que está siendo apoyada por grandes empresas de TI.

Finalmente, es importante destacar que el desarrollo del IoT no sólo pasa por el desarrollo de nuevos dispositivos o nuevas redes sino que también incluye el desarrollo de una nueva arquitectura de servicios. Se puede clasificar en tres los tipos de elementos que forman la arquitectura del IoT[5]:

- Hardware: como es lógico para la implementación del IoT se deben desarrollar o modificar todo tipo de componentes hardware y en especial los dispositivos de comunicación.
- Middleware: los datos enviados por los millones de dispositivos conectados al IoT deben ser almacenados y procesados en sistemas diseñados de forma adecuada para soportar la entrada de información de multitud de orígenes y la correcta identificación dato/dispositivo.
- Visualización: permite la presentación de la información obtenida. Provee la interfaz con el usuario final.

II. LoRa.

LoRa[15] es la capa física de la red LPWAN conocida como LoRaWAN. Como se ha indicado con anterioridad, Semtech es propietaria de LoRa mientras que la capa de acceso al medio (estrictamente LoRaWAN) se desarrolla de forma abierta por una entidad sin ánimo de lucro denominada *LoRa Alliance*.

Antes de proceder a realizar el estudio y valoración de LoRa se procederá a describir su arquitectura y topología. El conocimiento previo de estas características es fundamental para la correcta asimilación de alguno de los aspectos descritos a continuación.

Arquitectura y topología de la red LoRa.

La red LoRa está formada por tres elementos:

- Dispositivos finales (dispositivos clientes). Son los dispositivos utilizados para la conexión de los objetos a la red LoRa. Recogen la información específica del objeto y la transmiten a la pasarela.
- Pasarelas. Estaciones base LoRa que reciben las transmisiones realizadas por múltiples dispositivos finales y las reenvían a los servidores de red.
- Servidores de red. Equipos servidores encargados de la recepción y procesamiento de la información que proviene de los dispositivos finales así como de la gestión y configuración de la red y los dispositivos finales.

La red formada por los dispositivos finales y las pasarelas es de tipo estrella de un solo salto. Este tipo de redes son muy fáciles de implementar y gestionar (al no ser necesarios elementos de enrutamiento). Además las pasarelas, al no actuar como enrutadores, no retransmiten tráfico de otras pasarelas con el consiguiente ahorro energético. Sencillez y ahorro energético son requisitos esenciales en las redes de implementación del IoT.
Las pasarelas retransmiten la información que procede de los dispositivos finales a un servidor de red a través de una conexión IP estándar[10]. De esta forma las estaciones base funcionan a modo de puentes lo que resulta también en un diseño muy sencillo de la red y de sus componentes.

Se puede concluir que la red LoRa cumple con los requisitos de las redes LPWAN en cuanto a sencillez de implementación.

A. Formato de la trama física[2][19].

En la figura que sigue se puede ver el formato de la trama física de LoRa.

Figura 1: Formato de la trama física[11].

La trama comienza con un preámbulo de sincronización en el que se define el esquema de modulación del paquete[19]. Esto no sólo permite definir los parámetros de modulación de forma sencilla sino que además permite definir dichos parámetros de forma individualizada para cada paquete. Esto permite indicar el esquema de transmisión para cada paquete en función de la distancia a la pasarela (el objeto puede estar en movimiento) y por lo tanto ajustar el rendimiento y consumo eléctrico según las circunstancias. Algo de especial importancia en redes de implementación del IoT.

El preámbulo finaliza con un byte de sincronización que permite diferenciar entre las redes LoRa que están emitiendo en la misma banda de frecuencias de forma que un dispositivo sólo escucha las emisiones que tienen su mismo byte de sincronización[2], lo que permite la concurrencia de distintas redes LoRa en un mismo espacio.

El tamaño máximo del *payload* es de 255 bytes (dicho tamaño está definido por un solo byte en la cabecera de la trama) suficiente para la transmisión de datos de geolocalización, estado de dispositivo, información de sensores,…

El campo *PHYpayload* contiene la trama de la capa de acceso al medio LoRaWAN.

B. Modulación[9].

LoRa[14] opera en la banda ISM por debajo de 1 Ghz (en Europa se corresponde a las bandas 868 y 433 Mhz). Al ser una banda libre se puede usar sin licencia.

Utiliza como esquema de modulación de la señal un variación de la modulación DSSS de tipo *Spread Spectrum* denominada *Chirp Spread Spectrum (CSS)* que permite conexiones de bajo coste, bajo consumo (25 mA en transmisión y 10 mA en recepción[8]) robustas frente a interferencias y resistentes al efecto Doppler. Tal y como se vio en un apartado anterior, el uso de este tipo de esquema de modulación implica una mayor complejidad de los dispositivos de

comunicación y esto puede repercutir en el precio de los mismos lo que puede suponer un problema en redes de cientos de miles de dispositivos.

LoRa utiliza un método de ajuste dinámico de la potencia de emisión y la tasa de transferencia denominado ADR (*Adaptative Data Rate*) que principalmente permite al dispositivo final o a la red el ajuste dinámico de los parámetros antes citados en función de la distancia que separa al dispositivo final de la pasarela y del tamaño del mensaje[11]. El objetivo perseguido es que las comunicaciones sean energéticamente eficientes empleado la máxima velocidad posible.

Con el fin de mejorar la eficiencia en el uso del espectro y la capacidad de la red[7] LoRa permite seleccionar entre seis factores ortogonales de ensanchamiento (en adelante SF de S*preading Factor*) numerados del 7 al 12 en los que para cada uno se define una relación entre potencia y tasa de transferencia. A mayor SF, mayor es la sensibilidad del receptor y por lo tanto mayor el alcance del enlace por contra la velocidad del enlace decrece. En concreto la velocidad del enlace varía desde 0.3 kbps para un SF de 12, hasta 5486 kbps para un SF de 7 [9]. La sensibilidad de recepción varía entre -137dBm para un SF de 12 y -123 dBm para un SF de 7[9] lo que, como se ha comentado con anterioridad, tiene un impacto directo sobre el alcance de la conexión siendo el máximo de 14 km para un SF de 12 y de 2 km para un SF de 7[10].

C. Ciclo de trabajo.

La legislación europea actual impone restricciones en el ciclo de trabajo de las señales ISM menores de 1Ghz. En el caso de dispositivos finales, el ciclo de trabajo queda limitado al 1%. Esto, lógicamente, impone fuertes restricciones en el número de transmisiones diarias que puede hacer un dispositivo[7].

LoRaWAN no utiliza ningún mecanismo específico de acceso al medio. Se confía en las restricciones impuestas por el ciclo de trabajo como mecanismo de arbitraje del acceso al medio[12]. Esto tiene dos vertientes[7]: por un lado se reduce la latencia y el consumo de energía (el dispositivo transmite sin más) además de simplificar los dispositivos de comunicación, pero por otro lado el rendimiento de la red se puede ver afectado debido a un aumento de la probabilidad de que se produzcan colisiones (y las retrasmisiones asociadas) tal y como ocurriría en una red ALOHA puro. Esto no sólo puede afectar gravemente al rendimiento de la red sino que puede hacer que LoRa no sea adecuado para aplicaciones que no sean tolerantes a latencias elevadas o variables[1] como es el caso de las aplicaciones en tiempo real.

En cualquier caso, las restricciones impuestas por el ciclo de trabajo ejercen un importante impacto en el número de paquetes por día que un dispositivo puede enviar. A medida que aumenta la distancia entre un dispositivo final y la estación base, baja la tasa de transferencia lo que aumenta el tiempo en que la señal está en el aire. Similar consideración se puede hacer respecto al tamaño del mensaje, cuanto más grande sea el mensaje mayor el tiempo en que la señal está en el aire. A mayor tiempo de la señal en el aire menor es el número de paquetes por día que un dispositivo puede enviar. Esto puede hacer que la red LoRa no sea adecuada para aplicaciones de alta demanda de trasmisión de paquetes. No obstante hay que considerar que cuanto más cerca esté el dispositivo final de la pasarela menor será el tiempo de la señal en el aire y por lo tanto mayor el número de paquetes que se puedan enviar por día, por lo que una aplicación podría ver satisfechos sus requisitos si el dispositivo final del que depende está suficientemente cerca de una pasarela, bien porque se sitúa de forma estática de esta forma o bien porque hay una alta densidad de pasarelas que hace que alguna de ellas este suficientemente cerca.

III. LoRaWAN[11]

Como se ha indicado con anterioridad, LoRaWAN es la capa de acceso al medio de la red LoRA.

La parte principal de esta sección es el estudio y valoración de los aspectos de mayor relevancia del protocolo LoRaWAN. Dicho estudio se va a realizar de forma descendente; comenzando por la descripción de aspectos de alto nivel y acabando con el estudio de los de más bajo nivel (trama). No es posible entender adecuadamente los aspectos de bajo nivel de LoRaWAN sin antes describir aspectos de funcionamiento de alto nivel. Esto es así dado que LoRWAN es una capa de acceso al medio compleja, en la que además de las cuestiones puramente relacionadas con el acceso al medio se implementan diversas funcionalidades: soporte a diversos tipos de dispositivos finales, la activación y configuración de dispositivos finales en la red y la implementación de medidas de seguridad relacionadas con la confidencialidad y la integridad de la información. Para la implementación de estas funcionalidades el protocolo LoRaWAN cuenta con un conjunto de

órdenes MAC que se intercambian entre los dispositivos finales y los servidores de red.

A. Clases LoRaWAN[11].

En la red LoRaWAN los dispositivos se dividen en clases según las funcionalidades que soportan, en concreto: la clase A, B y C. Todos los dispositivos deben cumplir con las funcionalidades descritas en la clase A y opcionalmente cumplir las de las clases B y/o C. Además, las tres clases pueden coexistir en la misma red y los dispositivos finales pueden cambiar su configuración entre clases.

Clase A.

La planificación de las transmisiones corre a cargo del propio dispositivo final. La recepción, que sólo está permitida después de una transmisión completada correctamente, está formada por dos ventanas separadas de recepción. Si en la primera ventana ya se han recibido los datos la segunda ventana se deshabilita.
Esta clase es la más eficiente desde un punto de vista energético y es adecuada para aplicaciones que prácticamente sólo requieran enviar datos.

Clase B.

Esta clase permite la creación de ventanas de recepción sin la necesidad de que se produzca una trasmisión previa. Se aumenta pues la capacidad del dispositivo final de recibir datos. Mediante el envío de *beacons* por parte de la pasarela, ésta se sincroniza con el dispositivo final con el fin de planificar el tiempo en el que el dispositivo debe abrir la ventana de recepción.
La consecuencia inmediata de este aumento de la capacidad de recepción es el aumento del consumo eléctrico en el dispositivo final debido al coste energético del mecanismo de sincronización.

Clase C.

Este tipo de dispositivos están en modo de recepción permanente que sólo se interrumpe cuando se produce una transmisión. Esta clase de dispositivo presenta la mejor latencia de conexión entre los dispositivos finales y las pasarelas a cambio de un mayor consumo.

Las clases representan un balance entre consumo energético y capacidad de recepción. De esta forma se intentan perfilar los dispositivos en función de tres tipos de aplicaciones: las que prácticamente no necesitan enviar datos al dispositivo final, las que tienen una demanda media y finalmente las que tienen gran demanda de envío de datos al dispositivo final. Las clases son un ejemplo más del buen diseño de LoRaWAN dado que de una forma muy sencilla permiten indicar el perfil de consumo energético de un dispositivo.

En la clase de dispositivos B se introduce además la posibilidad de enviar tráfico de tipo *multicast* lo que permite dar soporte a aplicaciones que requieren este tipo de tráfico, así como la posibilidad de realizar *pings*.

B. Órdenes MAC[11].

Como se ha comentado con anterioridad, la capa de acceso al medio LoRaWAN es una capa compleja que implementa funcionalidades que en otro tipo de redes se realizan en niveles superiores como por ejemplo la autorización del uso de la red a los dispositivos finales o la seguridad.

Mediante una serie de órdenes que se intercambian entre el dispositivo final y el servidor de red se puede, por ejemplo, ajustar los parámetros del ADR, el valor máximo de EIRP, testear el estado de los dispositivos o ajustar los parámetros de conexión. De esta forma desde los servidores de red se puede, de manera centralizada, configurar los parámetros esenciales de conexión de los dispositivos lo que permite un ajuste dinámico de la red. Teniendo en cuenta que estas redes, en teoría, deben soportar cientos de miles de dispositivos y que estos pueden estar funcionando durante años, resulta absolutamente esencial el poder contar con el ajuste dinámico de la red antes mencionado.

C. Activación del dispositivo final[11].

Como ya se ha comentado, la seguridad es un elemento fundamental del IoT. En LoRaWAN no se deja esta cuestión a las capas superiores sino que se implementa soluciones de seguridad de manera muy eficaz en la propia capa de acceso al medio.

La conexión de un dispositivo a una red es uno de los primeros aspectos relacionados con la seguridad que deben ser tratados. Sólo los dispositivos autorizados deben poder unirse a una red más si tenemos en cuenta la naturaleza de la redes LoRaWAN, infinidad de dispositivos geográficamente dispersos.

En LoRaWAN se establece un mecanismo seguro por el que se autoriza a un dispositivo final a unirse a una red, este mecanismo se denomina

registro y activación de un dispositivo final en una red LoRaWAN.

El proceso de registro y activación finaliza con el almacenamiento en el dispositivo de los siguientes parámetros: dirección del dispositivo (*DevAddr*), identificador de aplicación (*AppEUI*), llave criptográfica de sesión (*NwkSKey*) y llave criptográfica de sesión de aplicación (*AppSKey*).

Hay dos procedimientos para realizar el proceso de configurar y registro de los dispositivos finales denominados métodos de activación: *Over-The-Air-Activation (OTAA)* y *Activation By Personalization (ABP)*.

c.1 Over-The-Air-Activation (OTAA)

El dispositivo final debe seguir un procedimiento de conexión con la red para poder participar en la misma. En el dispositivo final se debe configurar de manera manual con una serie de parámetros necesarios para el procedimiento de conexión, que son: un identificador global único (*DevEUI*) que identifica de forma única al dispositivo utilizando el esquema IEEE EUI64, el identificador de aplicación (*AppEUI*) y una llave criptográfica AES-128 (*AppKey*) específica para el dispositivo de la que se derivará la llave de sesión y la llave de sesión de aplicación.

El procedimiento de activación comienza con el envío por parte del dispositivo final de un mensaje MAC de petición de unión, denominado *join-request*, que contiene los parámetros *AppEUI* y *DevEUI* más un parámetro denominado *DevNone* que es un valor aleatorio utilizado para evitar ataques de reenvío de peticiones de unión. El servidor de red responde con un mensaje MAC de aceptación de unión, *join-accept*, si el dispositivo final tiene permitido el unirse a la red. El mensaje de aceptación está formado principalmente por los siguientes campos: un valor aleatorio (*AppNonce*) del que, junto con A*ppKey,* se derivan las dos llaves de sesión, la dirección del dispositivo (*DevAddr*) y el identificador de la red (*NetID*). Una vez recibido el mensaje de aceptación, el dispositivo final genera las llaves de sesión (*AppSKey* y *NwkSKey*) que junto al resto de parámetros son almacenados en el dispositivo final. A partir de ese momento ya puede realizar trasmisiones.

c.2 Activation By Personalization.

En el dispositivo final se configura de forma manual la dirección del dispositivo y las dos llaves de sesión de forma que el dispositivo puede transmitir desde el primer momento.

D. Seguridad en LoRaWAN[20].

El esquema de seguridad empleado en LoRaWAN provee a la red de mecanismos de autenticación mutua, integridad y confidencialidad, basado en un esquema de llave simétrica.

El proceso de activación de un dispositivo final en una red LoRaWAN se lleva a cabo a través de un mecanismo de autenticación mutua entre dispositivo final y servidor de red. Sólo los dispositivos autorizados pueden activarse en una determinada red. Durante el proceso de activación el dispositivo final utiliza la *AppKey* para calcular el MIC (*message integrity code*) del mensaje que es enviado al servidor como petición de conexión a la red. El servidor final, que tiene almacenada también la *AppKey* del dispositivo final, comprueba la autenticidad del mensaje mediante el uso de dicha llave. El servidor responde con un mensaje de aceptación cuyo MIC se calcula con la *AppKey* compartida, además el mensaje de aceptación se cifra con la propia *AppKey*, de esta forma el dispositivo final puede comprobar la autenticidad del mensaje.

Todo el tráfico entre un dispositivo final y un servidor de red se cifra y se firma mediante la utilización combinada de dos llaves: la llave de sesión de aplicación *AppSkey* y la llave de sesión de red *NwkSkey*. Ambas llaves se derivan de la llave *AppKey* y sólo son conocidas por un dispositivo final concreto y el servidor de red.

LoRaWAN confía la seguridad a un mecanismo de cifrado simétrico de llave compartida. En este tipo de sistemas se utiliza la misma llave para cifrar y descifrar la información, lo que implica que ambos lados del proceso deben conocer dicha llave. Los esquema de cifrado simétrico presenta un menor coste computacional que los de cifrado asimétrico, lo que los hace más adecuados para sistemas empotrados, pero como contrapartida hay que distribuir la llave compartida, y esta distribución se debe hacer de manera confidencial. Esto puede suponer un problema de seguridad. LoRaWAN resuelve esta problemática mediante la creación de las llaves de cifrado como derivación de una llave inicial (que sí puede ser vulnerable al tener que ser distribuida) junto a un valor aleatorio (que se crea durante el proceso de activación por lo que sólo es conocido por el dispositivo final y el servidor de red), que hace que el proceso de creación de las llaves no sea reproducible ni siquiera sabiendo el valor de la llave inicial. De esta sencilla forma se asegura la confidencialidad de la información dado que las claves de cifrado sólo están y han estado disponibles en el dispositivo final y el servidor de red.

La interceptación de la llave inicial no tiene consecuencias sobre la confidencialidad de las comunicaciones y sólo podría ser utilizada para la activación fraudulenta de un dispositivo en una determinada red. El algoritmo de cifrado utilizado es AES-128bits que en la actualidad no es vulnerable a ataques por fuerza bruta y presenta una buena relación entre coste computacional y robustez.

Se puede afirmar que LoRa presenta un buen esquema de seguridad.

E. La trama MAC[11].

La trama LoRaWAN, que se corresponde a la trama MAC del conjunto de protocolos LoRa/LoRaWAN, se sitúa en el campo *payload (PHYPayload)* de la trama física o trama de radio.

Figura 2: Formato de la trama MAC[11].

La trama MAC está formada por tres campos: la cabecera de la trama MAC (*MHDR*), el *payload* (*MACpayload*) y un campo de integridad (MIC).

En la cabecera se identifica principalmente el tipo de mensaje que contiene *MACpayload*. Hay seis tipos de mensajes predefinidos que se pueden clasificar en mensajes de tipo *join* (utilizados durante el proceso de registro y activación de los dispositivos) y mensajes de tipo *Data* (utilizados para el envío de órdenes y datos de aplicación). Los mensajes de tipo *Data* pueden requerir la confirmación de recepción por parte del destino. Está última característica añade cierta fiabilidad a la red pero tiene que ser utilizada con mucha cautela. El uso no planificado de reconocimientos puede afectar gravemente al rendimiento de la red (dado que aumenta la probabilidad de que se produzcan colisiones), a la autonomía de los dispositivos (por un mayor consumo eléctrico) y al número de mensajes por día que un dispositivo puede enviar (debido a las restricciones impuestas por el ciclo de trabajo). El supuesto beneficio en cuanto a fiabilidad que se obtiene mediante el uso de reconocimientos entra en contradicción con la grave merma de fiabilidad que puede presentar una red saturada en gran medida por el uso de dichos reconocimientos [1]. Queda en entredicho pues la utilidad de dicha funcionalidad si no se realiza una planificación estricta de su uso.

Es de destacar que LoRaWAN permite la extensión del conjunto de mensajes mediante la inclusión de un tipo especial denominado *Propietary* que permite la implementación de mensajes no estándar por parte del desarrollador. Aspecto que dota a la capa de acceso al medio de gran flexibilidad.

En la siguiente figura se muestra la estructura del campo *MACPayload*.

Figura 3: Formato del campo MACPayload de la trama MAC[11].

La cabecera (*FHDR*) contiene principalmente la dirección del dispositivo final (*DevAddr*) y una serie de campos de gestión y control. Destacaremos el campo *FCtrl* que implementa, junto a otras, la llamada funcionalidad de trama pendiente (*FPending*). Esta funcionalidad sólo está disponible cuando es la pasarela el origen de la emisión y sirve para indicar al dispositivo final que ésta tiene más información que enviar y que abra una nueva ventana de recepción lo antes posible. Esta funcionalidad resulta de gran utilidad si por ejemplo se quiere dotar a un dispositivo de clase A de mayor capacidad de recepción. No obstante, esta es otra característica a usar con cautela dado que su uso puede comprometer la autonomía esperada de un dispositivo final, por lo que es recomendable que el uso de esta funcionalidad sea ocasional.

El campo *FRMPayload* contiene o bien órdenes MAC o bien información específica de las aplicaciones. Siempre se transmite cifrado mediante la llave *NwkSKey* o la llave *AppSKey* lo que asegura la confidencialidad de la información.

F. Factores que limitan las redes LoRaWAN.

En esta última sección se van a discutir una serie de factores que limitan la capacidad de las redes LoRaWAN y que deben ser tomadas en cuenta a la hora de implementar este tipo de redes.

f.1 Ciclo de trabajo y colisiones.

Según [1], en redes en las que prevalecen las transferencias de baja velocidad el rendimiento se ve limitado por el número de colisiones (transmisiones que coinciden en el tiempo, la frecuencia y el SF) mientras que en las redes en las que prevalecen las transferencias de alta velocidad el rendimiento se ve limitado por las restricciones impuestas por la normativa respecto del ciclo de trabajo (por la limitación en el número de tramas por día que un dispositivo puede emitir).

f.2 Número de dispositivos.

Otro factor que limita la capacidad de la red LoRaWAN es el número de dispositivos. Tanto en [1] como en [3] se llega a la conclusión de que el aumento de dispositivos tiene un fuerte impacto sobre el rendimiento de la red. Tal y como figura en [1] , el valor máximo de transferencia en bytes por hora y dispositivo para un *payload* de 10 bytes en una red de 250 dispositivos finales es de 3670 bytes mientras que si la red es de 5000 dispositivos esta cifra se reduce a 180 bytes.

Además, tal y como figura en [19] y también para redes de más de 5000 dispositivos por pasarela, el número de mensaje diarios que podría enviar un dispositivo final sería de 2, algo que limita los usos que se le podrían dar a esta red.

f.3 Distancia a la pasarela.

Tal y como figura en [7] y también en [3] la red LoRaWAN es altamente escalable; una sola pasarela puede conectar una elevadísima cantidad de dispositivos siempre y cuando los requerimientos de velocidad y capacidad sean bajos. No obstante, tal y como figura en [7], para que el rendimiento de la red no se vea afectado la mayoría de dispositivos deberían situarse cerca de la pasarela sobre todo aquellos de elevado tráfico. A medida que aumenta el número de dispositivos que están lejos de la pasarela decrece significativamente la fiabilidad de la red.

f.4 Uso de reconocimientos.

El uso no planificado de reconocimientos puede limitar la escalabilidad de la red[7] dado que las pasarelas también están limitadas por las restricciones del ciclo de trabajo y la continúa emisión de tramas de reconocimiento puede limitar el número de tramas de órdenes o datos que la pasarela puede enviar por día.

IV. Estado Actual: Dispositivos y productos.

La red LoRaWAN está todavía en fase de desarrollo por lo que no son muchos los productos y servicios disponibles.

A continuación se clasifican los distintos productos que se puede encontrar en el mercado.

A. Dispositivos finales.

En este apartado se realiza un análisis de los distintos dispositivos que permiten el desarrollo de dispositivos finales.

a.1 Transceptor LoRa.

Dispositivo formado por un solo circuito integrado que contiene el modulador LoRa y un amplificador. No incluye la antena ni el cristal. La pila del protocolo LoRaWAN se debe implementar en un microcontrolador externo (*MCU*).

Son varios los dispositivos de este tipo sobre los que destacan los transceptores de la familia SX12XX de Semtech, empresa propietaria de la tecnología LoRa. Podemos distinguir dos gamas de dispositivos:

- Transceptores simples: Se corresponden a la serie SX1272/73 con una sensibilidad de -137dBm y la serie SX1276/77/78/79 con una sensibilidad de -148dBm. Ambas series tiene una potencia de emisión de +20dBm.
- Transceptores avanzados: Se corresponden a los dispositivos SX1236 y SX1238. En este tipo de dispositivos se incorpora circuitería extra que permite automatizar el proceso de emisión y recepción de paquetes liberando al *MCU* de la realización de dichas tareas. El primero de ellos tiene una potencia de emisión de +20dBm y el segundo de +27dBm.

a.2 Front-end LoRa.

Dispositivo que añade a un transceptor la antena y el cristal. Se trata de una solución que permite simplificar el diseño de dispositivos LoRa.

Como ejemplo de este tipo de dispositivos el de la empresa Dorji Applied Technologies DRF1278F[23] basado en el transceptor SX1278 de Semtech.

a.3 Modem LoRa.

Dispositivo que junto al transceptor incluye circuitería que implementa la pila del protocolo LoRaWAN. Este tipo de dispositivos se controlan mediante un *MCU* externo a través de una interfaz de órdenes ASCII sobre UART. Como ejemplo de este tipo de dispositivo el de la empresa Microchip RN2483[22] que presenta una sensibilidad de -147dBm y una potencia de emisión de +14dBm.

a.4 System-on-Chip LoRa.

Dispositivo que integraría el transceptor, la antena, la pila del protocolo LoRaWAN y el *MCU* en un solo circuito integrado.

En la actualidad no hay todavía ningún dispositivo disponible de este tipo aunque hay un acuerdo de las empresas Semtech y STMicroelectronics para su desarrollo.

B. Pasarelas.

En la actualidad no hay demasiadas soluciones en el mercado. Las que hay las podemos clasificar en diseños basados en ordenadores de placa reducida y diseños *ad-hoc*. Todas las soluciones tienen en común el empleo del circuito concentrador LoRa SX1301[30] de la empresa Semtech que proporciona, bajo licencia de software libre, los drivers para Linux.

b.1 Pasarelas basadas en ordenadores de placa reducida.

Las pasarelas se forman a partir de ordenadores de placa reducida como Raspberry-pi , Banana-pi,… a los que se les conecta un módulo concentrador LoRA WiMOD iC880A de la empresa IMST[27].

La funcionalidad de pasarela LoRa se consigue mediante la instalación del software de pasarela *lora-gateway-bridge* del proyecto de software libre *LoRaServer*.

b.2 Dispositivos ad-hoc.

Son varios los dispositivos *ad-hoc* disponibles en el mercado. Todos ellos utilizan una distribución de Linux para sistemas embebidos denominado *Yocto* como sistema operativo base. Podemos destacar:

- Pasarela Wirnet Station 868 de la empresa Kerlink[28]. Con conexión a redes IP mediante Ethernet y 3G.
- Pasarela MultiConnect de la empresa Multitech[24]. Con conexión a redes IP mediante Ethernet, 4G-LTE, 3G y 2G.
- Pasarela LORIX ONE IP43/IP65 gateway. Con conexión a redes IP mediante Ethernet. Esta pasarela está preconfigurada con el software de pasarela de LORIOT[26].

C. Servidores de red e infraestructura.

Respecto a la implementación de los servidores de red encontramos dos soluciones: una basada en software libre denominada *LoRaServer*[25] y otra propietaria denominada *LORIOT*[26].

LORIOT es una solución completa, desde el nivel de *middleware* al de tratamiento de datos y gestión de la seguridad, basada en tres servicios[26]:

- *Network Server*: Servicio de gestión de la red LoRaWAN.
- *Application Server*: Servicio de gestión de aplicaciones, gestión de dispositivos y almacenamiento a largo plazo de información.
- *Join Server*: Servicio de gestión de la seguridad de la red que implementa funciones de provisión automática de llaves, gestión del ciclo de vida de las llaves y gestión del acceso a llaves.

Además, la empresa ofrece soluciones "llave en mano" para la implementación y gestión de la red LoRaWAN. La infraestructura de servicios LORIOT puede ser instalada en la nube utilizando servicios como Amazon AWS, Microsoft Azure o IBM Bluemix.

LoRaServer es una solución todavía en desarrollo que está formada por tres componentes:

- *Lora-gateway-bridge*. Este componente redirecciona los datos recogidos en las pasarelas LoRa hacia el servidor de red. Puede ser instalado en la propia pasarela o como servicio independiente.
- *Loraserver*. Realiza las funciones del servidor de red.
- *Lora-app-server*. Componente de gestión de la infraestructura de LoRa que principalmente gestiona la información de las aplicaciones.

Como se ha indicado con anterioridad, los distintos componentes están en fase de desarrollo y por ejemplo algunas funciones del servidor de red, como la gestión de ADR, están en fase experimental y otras, como el soporte a dispositivos de clase B, están por desarrollar.

V. Conclusiones.

El llamado IoT o la conexión de todo tipo de dispositivos a la red Internet representa una auténtica revolución, los objetos se convierte en elementos activos en el flujo de información en Internet. Para posibilitarlo es necesario el desarrollo tecnológico de nuevos dispositivos y nuevas redes de conexión, las llamadas LPWAN. Son varias las propuestas de diseño de LPWAN siendo LoRaWAN una de las que mayor aceptación tiene en la actualidad.

Son varios los aspectos que alejan a la red LoRaWAN de ser una solución completa de implementación del IoT; los problemas ya comentados que limitan la capacidad de la red, la

inadecuación de la misma para dar soporte a determinados tipos de tráfico y la falta de dispositivos finales utilizables para cualquier tipo de objeto.

No obstante, representa una primera aproximación real a lo que en un futuro será el IoT. Como es lógico, la red LoRaWAN puede seguir evolucionando y convertirse en una red que cumpla satisfactoriamente con todos los requisitos del IoT o servir como base a nuevos desarrollos que sí los cumplan plenamente.

REFERENCIAS.

[1] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melià-Seguí, T. Watteyne, "Understanding the Limits of LoRaWAN" , IEEE Communications Magazine. Disponible en: https://www.researchgate.net/publication/305683193_Understanding_the_limits_of_LoRaWAN, Enero 2017.

[2] A. Augustin, J. Yi, T. Clausen, W. Mark Townsley, "A Study of LoRa: Long Range & Low Power Network for the Internet of Things.", Sensors Journal, 16(9), 1466. Disponible en: https://www.mdpi.com/1424-8220/16/9/1466/pdf, 9 septiembre de 2016.

[3] O. Georgiou, U. Raza, "Low Power Area Network Analysis: Can LoRa Scale?", IEEE Wireless Communications Letters, vol:PP, Issue:99. Disponible en: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7803607, 2017.

[4] C. Goursaud, J. Gorce,"Dedicated networks for IoT: PHY/MAC state of art and challenges", EAI Endorsed Transactiones on the Internet of Things 10-2015, vol 15, Issue 1,e3. Disponible en: https://hal.archives-ouvertes.fr/hal-01231221/file/eai.26-10-2015.150597.pdf, Octubre 2015.

[5] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", Revista Future Generation Computer Systems, volumen 29 (2013) páginas 1645-1660. Disponible en: https://www.researchgate.net/publication/228095891_Internet_of_Things_IoT_A_Vision_Architectural_Elements_and_FutureDirections, 24 febrero de 2013.

[6] U. Raza, P. Kulkerni, M. Sooriyabandara, "Low Power Area Network: An overview" IEEE Communications Surveys & Tutorials. Disponible en: http://ieeexplore.ieee.org/ document/7815384/ ?reload=true, 16 Enero de 2017.

[7] K. Mikhaylov, J. Petaejaejaervi, T. Haenninen, "Analysis of the Capacity and Scalability of the LoRa Wide Area Network Technology.", European Wireless 2016; 22th European Wireless Conference. Disponible en: http://ieeexplore.ieee.org/document/7499263/, 18-20 Mayo 2016.

[8] K. E. Nolan, W. Guibene, M. Y. Kelly, "An Evaluation Of Low Power Wide Area Network Technologies For The Internet Of Things.", Wireless Communications and Mobile Computing Conference (IWCMC), 2016 International. Disponible en: http://ieeexplore.ieee.org/document/7577098/ , 5-9 Septiembre de 2016.

[9] Semtech Corporation, "AN1200.02. LoRa Modulation Basics.", Disponible en: http://www.semtech.com/images/datasheet/an1200.22.pdf, Mayo 2016.

[10] N. Ducrot, D. Ray, A. Saadani, O. Hersent, G. Pop, G. Remond, "LoRa Device Developer Guide", Disponible en: https://partner.orange.com/wp-content/uploads/2016/04/LoRa-Device-Developer-Guide-Orange.pdf, Abril de 2016.

[11] N. Sornin, M. Luis, T. Eirich, T. Kramp, O. Hersent, "LoRaWAN Specifications 1.0.2", www.lora-alliance.org, Julio de 2016.

[12] A.S. Tanenbaum, "The medium access sublayer" pp 243-338 en Computer Networks, 3rd ed, Prentice-Hall, 1996.

[13] S. Woelfflé, H. Sundmaeker, P. Guillemin, P. Firess, "Vision and challenges for realising the Internet of Things", Cluster of European Research projects on the Internet of Things- CERP-IoT, Marzo de 2010.

[14] www.lora-alliance.org

[15] www.semtech.com

[16] www.sigfox.com

[17] www.ingenu.com

[18] A. Minaburo, L. Toutain, *LPWAN GAP Analysis, draft-minaburo-lpwan-gap-analysis-01*, pp. 1-2, Network Working Group (2016). Disponible en https://tools.ietf.org/html/draft-minaburo-lpwan-gap-analysis-01

[19] D. Bankov, E. Khorov, A. Lyakhov, "On the Limits of LoRaWAN Channel Access". 2016 International Conference on Engineering and Telecommunication.

[20] Lora Alliance, "LoRaWAN Security. Full end-to-end encryption fot IoT Application providers". Disponibles en https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN_Security-Whitepaper_V6_Digital.pdf

[21] "LoRa SX1272/73 Datasheet, Rev 3.1, Marzo 2017". Disponible en http://www.semtech.com/images/datasheet/sx1272.pdf

[22] "Microchip RN2483 Datasheet. Revision C, Abril 2017". Disponible en http://ww1.microchip.com/downloads/en/DeviceDoc/50002346C.pdf.

[23] "Dorji Applied Technologies DRF1278F Datasheet V1.11. Disponible en

http://www.dorji.com/docs/data/DRF1278F.pdf.
[24] “MultiConnect Conduit Datasheet”. Disponible en http://www.multitech.com/documents/publications/data-sheets/86002170.pdf.
[25] https://docs.loraserver.io/loraserver/
[26] https://www.loriot.io/index.html
[27]”WiMOD iC880A Datasheet”. Disponible en: https://wireless-solutions.de/images/stories/downloads/Radio%20Modules/iC880A/iC880A_Datasheet_V0_17.pdf
[28] “Wirnet Station 868MHz datasheet”. Disponible en: http://www.kerlink.fr/en/products/lora-iot-station-2/wirnet-station-868
[29]”LORIX ONE user manual”. Disponible en: https://lorixone.io/telechargement/en/LORIX_One_user_manual_EN.pdf
[30]”SX1301 Datasheet”. Disponible en: http://www.semtech.com/images/datasheet/sx1301.pdf.