IoT: Dispositivos, tecnologías de transporte y aplicaciones

Antonio Jesús González García
Máster Universitario de Ingeniería de Telecomunicación UOC-URL
Telemática

José López Vicario
Xavi Vilajosana Guillen
11 Junio 2017

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

FICHA DEL TRABAJO FINAL

Título del trabajo:	IoT: Dispositivos, tecnologías de transporte y aplicaciones
Nombre del autor:	Antonio Jesús González García
Nombre del consultor/a:	José López Vizcaíno
Nombre del PRA:	Xavi Vilajosana Guillen
Fecha de entrega (mm/aaaa):	06/2017
Titulación::	Máster Universitario de Ingeniería de Telecomunicación UOC-URL
Área del Trabajo Final:	Telemática
Idioma del trabajo:	Castellano
Palabras clave	Arquitectura, Protocolo, Transporte.

Resumen del Trabajo (máximo 250 palabras): Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.

Desde la que Internet apareció en nuestras vidas, la sociedad ha cambiado sus formas de comunicarse e interrelacionarse. Internet de las cosas está cambiando la forma en que nos relacionamos y la forma en la que se relacionan los objetos o dispositivos de los que no rodeamos a diario. Existen multitud de tecnologías que se utilizan para poder conectar esos objetos a Internet, para controlar estos dispositivos y para transportar la información que generan. Desde un punto de vista práctico y sin pérdida de generalidad, IoT se estructura en tres planos o niveles, donde se utilizan y desarrollan las diferentes tecnologías que se analizan. Quizás lo más novedoso es el desarrollo de nuevas tecnologías para el despliegue de redes que puedan soportar la conexión de una gran cantidad de dispositivos. El desarrollo de estas nuevas redes, está haciendo reaccionar a los operadores de telefonía móvil, adecuando su infraestructura desplegada a los requisitos de los dispositivos, para no desaprovechar esta oportunidad de negocio.

Numerosos investigadores estudian nuevas tecnologías y arquitecturas para proporcionar un marco de desarrollo que estandarice las diferentes tecnologías e impulse más aun el despliegue de IoT. Se presentan en este proyecto las tecnologías más relevantes y aplicaciones que están haciendo posible el desarrollo e implantación de IoT y que en gran medida están empezando a influir en nuestras vidas.

Abstract (in English, 250 words or less):

Since the Internet appeared in our lives, society has changed its ways of communicating and interrelating. The Internet of things is changing the way we relate and the way in which objects or devices that we do not surround on a daily basis are related. There are many technologies that are used to connect these objects to the Internet, to control these devices and to transport the information they generate. From a practical point of view and without loss of generality, IoT is structured in three levels or levels, where the different technologies that are analyzed are used and developed. Perhaps the most novel is the development of new technologies for the deployment of networks that can support the connection of a large number of devices. The development of these new networks is reacting to mobile operators, adapting their deployed infrastructure to the requisitions of the devices, not to miss this business opportunity.

Numerous researchers are studying new technologies and architectures to provide a development framework that standardizes the different technologies and further impels IoT deployment. This project presents the most relevant technologies and applications that are making possible the development and implementation of IoT and that are largely beginning to influence our lives.

Índice

1. Introducción ... 1
1.1 Contexto y justificación del Trabajo ... 1
1.2 Objetivos del Trabajo ... 1
1.3 Enfoque y método seguido ... 1
1.4 Planificación del Trabajo ... 1
1.5 Breve sumario de productos obtenidos ... 3
1.6 Breve descripción de los otros capítulos de la memoria ... 3
2. ¿Qué es Internet de las cosas? ... 4
2.1 Arquitectura de IoT. ... 5
2.1.1. Arquitectura de tres niveles. ... 5
3. Dispositivos utilizados en IoT. ... 10
3.1. Sensores. ... 10
3.1.2. Físicos. ... 10
3.1.3. Químicos y bioquímicos. ... 11
3.2. Actuadores. ... 11
3.2.1. Motores. ... 11
3.2.2. Servomotores ... 11
3.2.3. Motores paso a paso (Steppers) ... 12
3.2.4. Electroválvulas. ... 12
3.3. Teléfonos móviles (smartphones) ... 12
4. Protocolos de comunicaciones. ... 14
4.1. Modelo OSI ... 15
4.2. Sistemas M2M capilares ... 15
4.2.1. Capa física y enlace. ... 16
4.2.1.1. IEEE 802.15.1 (Bluetooth) ... 16
4.2.1.2. RFID ... 16
4.2.1.3. Near Field Communication (NFC) ... 17
4.2.1.4. IEEE 802.11 (Wi-Fi) & 802.11 Low Power ... 17
4.2.1.5. Z-Wave ... 18
4.2.1.6. IEEE 802.15.4 ... 18
4.2.1.7. WirelessHART ... 19
4.2.1.8. Especificaciones LPWA. ... 20
4.2.2. Capa de red. ... 21
4.2.2.1. IETF 6LoWPAN ... 21
4.2.2.2. ZigBee ... 22
4.2.3. Capa de transporte. ... 23
4.2.4. Capa de sesión, presentación y aplicación. ... 24
4.2.4.1. HTTP ... 24
4.2.4.2. CoAP. ... 25
4.2.4.3. Message Queue Telemetry Transport (MQTT) ... 28
4.2.4.4. Extensible Messaging and Presence Protocol (XMPP). ... 29
4.2.4.5. Advanced Message Queuing Protocol (AMQP). ... 31
4.2.4.6. Data Distribution Service (DDS). ... 32
4.3. LPWA networks. ... 34
4.3.1. Técnicas de diseño. ... 37

4.3.2. Tecnologías LPWA a estudio: SigFox y LoRa 40
4.3.2.1. SigFox 40
4.3.2.2. LoRa. 43
4.3.3. Despliegue de redes LPWA en España. 45
4.4. Sistemas M2M celulares. 46
4.4.1 Tecnología 3GPP. 47
4.5 Opinión sobre las tecnologías expuestas. 48
4.5.1. Factores a tener en cuenta en la evaluación de tecnologías en el diseño de sistemas IoT. 49
5. Aplicaciones IoT 51
5.1. Áreas de aplicación. 51
5.1.1. Smart Home. 51
5.1.2. Smart City. 52
5.1.3. Agricultura y ganadería. 53
5.1.4. Wearables 54
5.1.5. Industrial IoT. 55
5.2. Consideraciones de diseño. 56
5.2.1. Objetivo de la aplicación. 57
5.2.2. Tamaño. 58
5.2.3. Requisitos de comunicación. 58
5.2.4. Fuente de energía. 58
5.2.5. Consideraciones ambientales. 58
5.2.6. Comunicación con otros productos. 58
5.3. El impacto del internet de las cosas en nuestra sociedad. 59
5.3.1. El impacto directo sobre las personas. 59
5.3.2. Hacia un nuevo modelo de negocio más colaborativo. 60
6. Conclusiones. 62
7. Glosario. 63
8. Bibliografía 64

Lista de figuras

ILUSTRACIÓN 1: ARQUITECTURA DE 3 Y 5 NIVELES 5
ILUSTRACIÓN 2: CLOUD COMPUTING 7
ILUSTRACIÓN 3: FOG COMPUTING 8
ILUSTRACIÓN 4: ARQUITECTURA SIOT 8
ILUSTRACIÓN 5: INICIATIVAS ARQUITECTURA DE REFERENCIA 9
ILUSTRACIÓN 6: DE IZQUIERDA A DERECHA: SENSOR DE TEMPERATURA TMP36, LDR, SENSOR DE INCLINACIÓN 10
ILUSTRACIÓN 7: ESQUEMA SENSOR BIOQUÍMICO 11
ILUSTRACIÓN 8: SERVOMOTORES. 12
ILUSTRACIÓN 9: MOTOR PASO A PASO. 12
ILUSTRACIÓN 10: ELECTROVÁLVULAS DE VACÍO DE 2 VÍAS, DE ACCIONAMIENTO DIRECTO. 12
ILUSTRACIÓN 11: LOS DATOS BAJAN POR LA PILA OSI DEL DISPOSITIVO EMISOR Y SUBEN POR LOS DEL DISPOSITIVO RECEPTOR 15
ILUSTRACIÓN 12: ETIQUETA RFID 17
ILUSTRACIÓN 13: ZIGBEE WIRELESSHART Y OSI 19
ILUSTRACIÓN 14: COMPARACIÓN DE PROTOCOLOS 20
ILUSTRACIÓN 15: OSI VS SIGFOX VS LORA 20
ILUSTRACIÓN 16: COMPARATIVA 6LOWPAN Y LOW-POWER WI-FI 22
ILUSTRACIÓN 17: ENTORNO COAP 26
ILUSTRACIÓN 18: TIPOS DE RESPUESTAS 27
ILUSTRACIÓN 19: ARQUITECTURA DE MQTT 29
ILUSTRACIÓN 20: MENSAJE MQTT. 29
ILUSTRACIÓN 21: COMUNICACIONES EN XMPP 30
ILUSTRACIÓN 22: ESTRUCTURA DE UNA STANZA XMPP 31
ILUSTRACIÓN 23: ARQUITECTURA AMQP. 31
ILUSTRACIÓN 24: FORMATO DE LA TRAMA AMQP 32
ILUSTRACIÓN 25: MODELO CONCEPTUAL DE DDS 34
ILUSTRACIÓN 26: COMPARACIÓN PROTOCOLOS NIVEL APLICACIÓN 34
ILUSTRACIÓN 27: CARACTERÍSTICAS DE LAS REDES LPWA 35
ILUSTRACIÓN 28: COMPARACIÓN ENTRE UNB Y SPREAD SPECTRUM. 38
ILUSTRACIÓN 29: USO DE ANCHO DE BANDA 41
ILUSTRACIÓN 30: PILA DE PIOCOLOS SIGFOX COMPARADA CON EL MODELO OSI 42
ILUSTRACIÓN 31: ARQUITECTURA SIGFOX 43
ILUSTRACIÓN 32: LORA Y LORAWAN DENTRO DEL MODELO OSI 43
ILUSTRACIÓN 33: ARQUITECTURA LORA 44
ILUSTRACIÓN 34: CARACTERÍSTICAS LORA, SIGFOX 45
ILUSTRACIÓN 35: DESPLIEGUE DE LA RED DE CELLNEX-TELECOM 46
ILUSTRACIÓN 36: TECNOLOGÍAS EXPUESTAS EN LA PILA ISO 48
ILUSTRACIÓN 37: TASA DE DATOS Y ALCANCE 50
ILUSTRACIÓN 38: SMART HOME 51
ILUSTRACIÓN 39: SMART CITY 52
ILUSTRACIÓN 40: CITY OS 53
ILUSTRACIÓN 41: SMART AGRICULTURE 54
ILUSTRACIÓN 42: WEARABLE TECHNOLOGY 54
ILUSTRACIÓN 43: IIOT 55
ILUSTRACIÓN 44: CONSIDERACIONES DE SEGURIDAD 57

1. Introducción

1.1 Contexto y justificación del Trabajo

Internet de las cosas (IoT) se ha desarrollado a partir de la convergencia de una serie de tecnologías, que han evolucionado de forma independiente desde su concepción. En Internet de las Cosas las cosas (objetos) tienen conexión a Internet en cualquier momento y lugar. En un sentido técnico, consiste en la integración de sensores y dispositivos dentro de objetos cotidianos que quedan conectados a Internet a través de redes fijas e inalámbricas. El hecho de que Internet esté presente al mismo tiempo en todas partes permite que la adopción masiva de esta tecnología sea más factible. Dado su tamaño y coste, los sensores son fácilmente integrables en hogares, entornos de trabajo y lugares públicos. De esta manera, cualquier objeto se puede conectar y manifestarse en la Red. Además, IoT implica que todo objeto puede ser una fuente de datos. Esto está empezando a transformar la forma de hacer negocios, la organización del sector público y el día a día de millones de personas.

Este proyecto muestra la panorámica actual de las tecnologías más utilizadas en IoT, los modelos de aplicación y su impacto en nuestra vida cotidiana.

1.2 Objetivos del Trabajo

- Proporcionar una visión general de IoT mostrando su arquitectura y componentes.
- Presentar los diferentes dispositivos utilizados en IoT.
- Introducir las diferentes plataformas y tecnologías lpwa.
- Comparar las implementaciones de sigfox y LoRa.
- Comprobar el despliegue actual de las redes lpwa.
- Analizar las diferentes aplicaciones y su impacto en nuestras vidas.

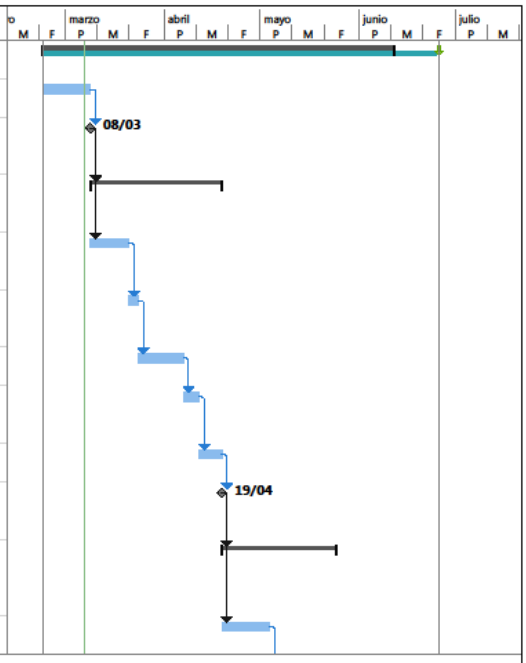
1.3 Enfoque y método seguido

El proyecto muestra lo que es y consiste Internet de las cosas, a través de las diferentes tecnologías que actualmente se utilizan, describiendo sus características extraídas de los diferentes estudios y publicaciones existentes, de esta forma se han desarrollado los objetivos establecidos. Estas tecnologías se plasman en tres planos o niveles: dispositivos, transporte y aplicaciones.

1.4 Planificación del Trabajo

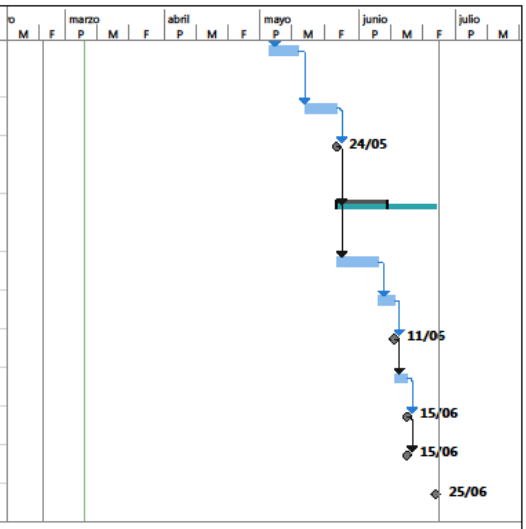
En la planificación del trabajo se han definido diferentes hitos que coinciden con las diferentes entregas (PECs). Para cada una de las entregas se han respetado escrupulosamente los plazos planteados en la planificación, a partir de la segunda entrega se ha revisado el planteamiento con los consejos aportados por el consultor, aportando puntos de vista desde el punto de vista profesional.

Id		Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1			**TFM-Telemática**	**81 días**	**mié 22/02/17**	**dom 11/06/17**
2			Planificación	11 días	mié 22/02/17	mié 08/03/17
3			PEC1 : Entrega de la planificación del trabajo	0 días	mié 08/03/17	mié 08/03/17
4			**Busqueda de información y redacción**	**30 días?**	**jue 09/03/17**	**mié 19/04/17**
5			Tecnología de sensores y actuadores	9 días?	jue 09/03/17	lun 20/03/17
6			Analisis y sintesis de la información	3 días	mar 21/03/17	jue 23/03/17
7			Tecnologias de transporte	10 días?	vie 24/03/17	jue 06/04/17
8			Analisis y sintesis de la información	3 días?	vie 07/04/17	mar 11/04/17
9			Redacción PEC2	5 días?	mié 12/04/17	mar 18/04/17
10			PEC2:Primera entrega del proyecto	0 días	mié 19/04/17	mié 19/04/17
11			**Busqueda de información aplicaciones y redacción**	**27 días?**	**mié 19/04/17**	**mié 24/05/17**
12			Aplicaciones	12 días?	mié 19/04/17	mié 03/05/17



Página 1

Id		Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
13			Analisis y sintesis de la información	7 días?	jue 04/05/17	vie 12/05/17
14			Redacción PEC3	8 días?	lun 15/05/17	mié 24/05/17
15			PEC3: Segunda entrega del proyecto	0 días?	mié 24/05/17	mié 24/05/17
16			**Redaccion del proyecto y presentación**	**12 días?**	**jue 25/05/17**	**vie 09/06/17**
17			Redacción final	9 días	jue 25/05/17	mar 06/06/17
18			Revisión	4 días	mié 07/06/17	dom 11/06/17
19			Entrega de la memoria final	0 días?	dom 11/06/17	dom 11/06/17
20			crear presentación	4 días	lun 12/06/17	jue 15/06/17
21			Entrega de la presentación	0 días	jue 15/06/17	jue 15/06/17
22			Inicio del tribuna	0 días	jue 15/06/17	jue 15/06/17
23			Final del tribunal	0 días	dom 25/06/1	dom 25/06/17



Página 2

1.5 Breve sumario de productos obtenidos

El resultado es una muestra de los tipos de dispositivos, protocolos de transporte y aplicaciones más relevantes que actualmente se utilizan en IoT, proporcionado una serie de factores o consideraciones a tener en cuenta en la elección de tecnologías en el diseño de sistemas de IoT.

1.6 Breve descripción de los otros capítulos de la memoria

En el capítulo 2 se proporciona una definición y una visión general de Internet de las cosas. Se presentan algunas de las arquitecturas existentes.

En el capítulo 3 se muestran los diferentes tipos de dispositivos utilizados en IoT.

En el capítulo 4 se introducen los diferentes protocolos de comunicaciones utilizados en IoT, se realiza un recorrido por las diferentes capas mostrando donde se ubican cada uno. También se introducen diferentes tecnologías LPWA y se dan a conocer con mayor nivel de detalle dos de ellas. Se muestran algunas tecnologías desarrolladas como respuesta a las LPWA y por último se presentan opiniones sobre las tecnologías expuestas y factores o consideraciones para la elección de las mismas.

En el capítulo 5, se muestran distintas aplicaciones de IoT, consideraciones a tener en cuenta en el desarrollo de aplicaciones y el impacto que IoT está teniendo en nuestras vidas y en la forma de hacer negocios.

Por último, en el capítulo 6 se muestran las conclusiones.

2. ¿Qué es Internet de las cosas?

Internet de las cosas, (IoT) abarca una serie de dispositivos y tecnologías que junto a Internet, omnipresente en todos los rincones del mundo, está afectando a nuestra vida cotidiana de formas inimaginables. Vivimos en una era en la que la una gran variedad de dispositivos están conectados a través de Internet, y por ende, entre si.

Internet de las Cosas es una realidad muy presente que está evolucionando a pasos agigantados. Millones de dispositivos están siendo conectados entre sí a través de distintas redes de comunicación. Pequeños sensores permiten medir desde la temperatura de una habitación hasta el tráfico de taxis en una ciudad. A diario, cámaras de vigilancia velan por la seguridad en los edificios y los paneles del metro nos indican el tiempo que falta hasta la llegada del siguiente tren. Incluso en las multas de tráfico existe poca intervención humana. Cada vez más objetos están siendo integrados con sensores, ganando capacidad de comunicación, y con ello las barreras que separan el mundo real del virtual se difuminan.

El termino IoT ha sido definido por diferentes Autores en muchas formas diferentes, Vermesan et al. [1] definen Internet de las cosas, simplemente como una interacción entre lo físico y lo digital. El mundo digital interactúa con el mundo físico usando una plétora de sensores y actuadores. Otra definición [2] define Internet de las cosas como un paradigma en el que la capacidad de cómputo y comunicación están incrustadas en cualquier tipo de objeto concebible. Existe múltiples definiciones [3] de IoT, que abarcan desde pequeños sistemas localizados, restringidos a una ubicación específica hasta un gran sistema global distribuido, compuesto por varios sistemas complejos.

IoT, no es una idea nueva, Mark Weiser, director científico del Xerox Palo Alto Research Center, introdujo el concepto de computación ubicua, a principios de los 90. Weiser abogaba por un futuro en el que la computación formaría parte integral de nuestra vida diaria y resultaría transparente para nosotros. Weiser no acuñó el término IoT, que se atribuye al Auto-ID Center del Massachusetts Institute of Technology (MIT) a finales de los años noventa. Sin embargo, la idea del IoT ha tomado relevancia práctica gracias a la rápida evolución de la electrónica durante la última década.

Esta evolución ha seguido el patrón marcado por Gordon Moore, cofundador del fabricante de microprocesadores Intel. Moore formuló en 1965 su famosa predicción, conocida a nivel mundial como Ley de Moore, que fue refinada en 1975, en ella establece que el número de transistores que contiene un chip se duplica cada dos años aproximadamente. Bien sea porque Moore fue capaz de predecir el futuro o porque los fabricantes de procesadores fijaron sus palabras como un objetivo a largo plazo, la Ley de Moore se ha venido cumpliendo durante los últimos cuarenta años.

Funciones que décadas atrás requerían de un ordenador del tamaño de una habitación, son hoy día realizadas con facilidad por simples dispositivos electrónicos del tamaño de una gota de agua. El tamaño, el coste y el consumo de energía del hardware se han reducido drásticamente, por lo que ahora es posible fabricar dispositivos electrónicos diminutos a un coste muy reducido.

Estos pequeños dispositivos, junto con la expansión de las redes de comunicación, permiten incorporar inteligencia y conexión a los objetos del mundo real y están transformando lo que era una red global de personas en una red global de todas las cosas.

En este contexto podemos dar una definición de los que es y representa IoT: Internet de las cosas es una nueva forma de entender Internet, que aglutina un gran número de tecnologías que han evolucionado desde su nacimiento de forma independientemente, junto con nuevas tecnologías, ya en desarrollo o por desarrollar, que permite a pequeños dispositivos electrónicos interactuar con su entorno, bien recogiendo información del mismo o produciendo acciones para modificarlo.

2.1 Arquitectura de IoT.

Aunque se han propuesto diferentes arquitecturas para IoT, no existe un consenso generalizado, diferentes investigaciones han propuesto modelos de arquitectura que recogen con mayor o menor detalle los diferentes aspectos de IoT. A continuación se muestran algunas de las arquitecturas más relevantes.

2.1.1. Arquitectura de tres niveles.

Una de las arquitecturas más básicas, es la arquitectura de tres niveles: Nivel de percepción, nivel de red y nivel de aplicación.

- El nivel de percepción es el nivel físico, donde los sensores recogen información del entorno.
- El nivel de red es el responsable de conectar los sensores y servidores entre sí para transmitir y procesar los datos recogidos por los sensores.
- El nivel de aplicación es donde IoT puede ser desplegado en diferentes áreas de aplicación.

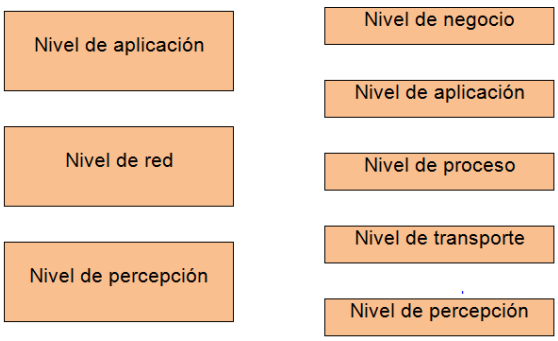


Ilustración 1: Arquitectura de 3 y 5 niveles

2.1.2. Arquitectura de cinco niveles.

Formada por los niveles de percepción, transporte, proceso, aplicación y nivel de negocio. En este modelo de arquitectura los niveles de percepción y aplicación son los mismos que en la arquitectura de tres niveles. En cuanto al resto de niveles:

- El nivel de transporte, transfiere los datos los datos de los sensores mediante redes 3G, LAN, Bluetooh, RFID y NFC, desde el nivel de percepción al nivel de proceso y viceversa.
- El nivel de proceso almacena, analiza y procesa grandes cantidades de datos procedentes del nivel de percepción. Puede proporcionar y gestionar servicios los niveles más bajos utilizando tecnologías de bases de datos, cloud computing y big data.
- El nivel de negocio gestiona las aplicaciones, el modelo de negocio y la privacidad.

2.1.3. Otras arquitecturas.

Además de las dos comentadas, existen en la literatura otras arquitecturas que recogen aspectos más concretos de IoT. A continuación se mencionarán algunas de las propuestas por diferentes investigadores.

2.1.3.1. Arquitecturas basadas en cloud y fog.

Ambas se basan en la naturaleza de los datos generados por IoT. La arquitectura en cloud se basa en procesar los datos en infraestructuras en la nube manteniendo la infraestructura de procesamiento en el centro, las aplicaciones encima y la infraestructura de dispositivos debajo. En la arquitectura fog los datos son procesados localmente en dispositivos inteligentes en lugar de ser enviados a la nube.

2.1.3.1.1 Cloud computing.

El National Institute of Standards and Technology (NIST) [4] define el cloud computing como:

> "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

Tal como establece el NIST, este modelo está compuesto de las siguientes características:

- Servicios bajo demanda: el cliente puede utilizar recursos, como tiempo de servidor y almacenamiento, a medida que los necesita de forma automática sin intervención humana.
- Accesibilidad: gracias a las nuevas tecnologías, los capacidades de computo en el cloud se encuentran liberados en la red y disponibles

para los usuarios, que pueden acceder a ellos a través de mecanismos estándar que permiten usar gran variedad de clientes (PDAs, teléfonos móviles,...)

- Conjuntos de recursos: Los recursos son agrupados en pooles, para dar servicio a diferentes clientes reasignando los diferentes recursos, ya sean físicos o virtuales, de acuerdo con la demanda. El cliente, normalmente, no tiene conocimiento de la localización exacta de los recursos pero puede especificarla a un mayor nivel de abstracción (país, región o datacenter). Ejemplos de recursos van desde almacenamiento, pasando por capacidad de proceso, memoria, red, ancho de banda y maquinas virtuales.
- Elasticidad y escalabilidad: las aplicaciones en cloud son totalmente elásticas en cuanto a su rapidez de implementación y adaptabilidad. Además, de que son totalmente escalables y adaptables a las necesidades del cliente, el proveedor y la tarifa de suscripción.
- Supervisión del servicio: los sistemas en cloud controlan y optimizan el uso de los recursos de manera automática, por lo que el uso de estos puede seguirse, controlarse y notificarse.
- Seguridad: en residir los datos en empresas certificadas por la gestión de la información, tenemos una garantía muy alta que los datos se encuentran fuera de peligro.

Ilustración 2: cloud computing

Sin entrar en más detalles sobre cloud computing, podemos decir que aunque, IoT y cloud computing han seguido, en el pasado, una evolución independiente, las características del cloud computing, hacen que este paradigma de computación sea atractivo para IoT. Pueden identificarse muchas ventajas de la integración de IoT y cloud computing [5]. La ventaja más palpable es que cloud computing puede ofrecer recursos, virtualmente ilimitados a IoT para así compensar las restricciones tecnológicas de los dispositivos que componen los sistemas IoT.

2.1.3.1.2 Fog computing.

Aunque fog computing [6] tiene como punto de partida el cloud computing, es un modelo que se basa en concentrar datos y aplicaciones en los dispositivos al borde de la red. Los datos son procesados localmente en un dispositivo inteligente en lugar de ser enviados, sin procesar, a través de la red. Fog, al igual que cloud, proporciona a los usuarios finales, datos, cálculo, almacenamiento y servicios.

Las principales características de fog computing son:

- Los datos y las aplicaciones se sitúan en el borde de la red.
- Almacenamiento y computación distribuidos.
- Alta distribución geográfica de un gran número de dodos.
- Heterogeneidad de dispositivos, datos y aplicaciones.
- Comunicaciones en tiempo real y movilidad.

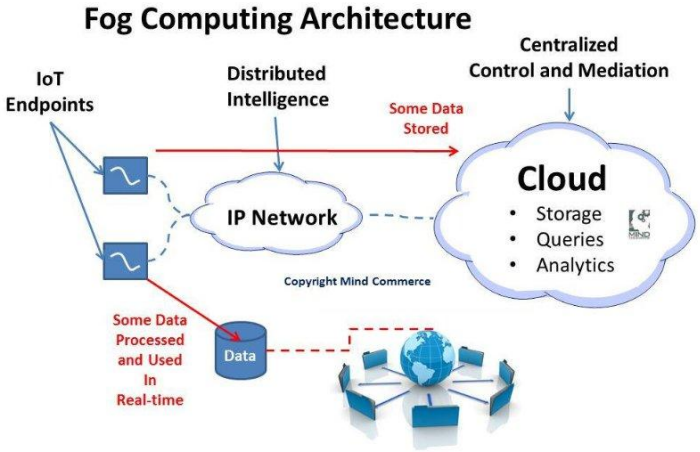


Ilustración 3: fog computing

2.1.3.2. Social IoT.

Social IoT (SIoT) [7] hace referencia a la convergencia de las redes sociales e IoT [8], para la creación de redes sociales en la que los dispositivos son nodos, que establecen enlaces sociales de la misma forma que lo hacen las personas. Este concepto está ganando rápidamente adeptos gracias a los beneficios derivados del potencial de las redes sociales dentro del dominio de IoT, como puede ser la facilidad de navegación en una red dinámica compuesta por millones de objetos, gestión de la confianza entre dispositivos, cuando se intercambian información y descubrimiento de servicios e información eficientes. Representa un ecosistema que permite a personas y dispositivos interactuar entre sí. La arquitectura se compone de:

- Nivel destinado a la adquisición de datos y colaboración de nodos en redes de área local de corto alcance
- Nivel de red, que transfiere los datos a través de diferentes redes.
- Nivel de aplicación.

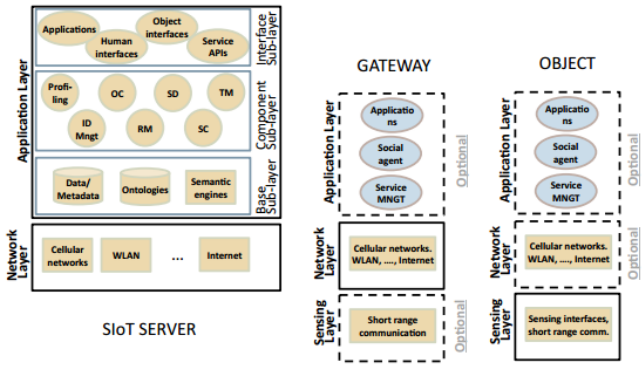


Ilustración 4: Arquitectura SIoT

Hasta aquí se han presentado diferentes arquitecturas de IoT. Podríamos seguir presentando diferentes arquitecturas moviendo el plano de proceso hacia los dispositivos sensores o actuadores, o utilizando dispositivos sin "inteligencia", dejando el proceso en el plano de aplicación….

Existen diferentes iniciativas para definir una arquitectura de referencia que de alguna manera estandarice los diferentes protocolos, facilite la interoperabilidad, simplifique el desarrollo y permita una implementación fácil.

En la tabla siguiente se muestran algunas de estas iniciativas:

Nombre	Dirección web
Reference Architecture Model Industrie 4.0 (RAMI 4.0)	www.zvei.org/en/association/specialist - divisions/automation/Pages/default.aspx
Industrial Internet Reference Architecture (IIRA)	www.iiconsortium.org
Internet of Things— Architecture (IoT-A)	www.iot-a.eu/public/public-documents/d1.5/view
Standard for an Architectural Framework for the Internet of Things (IoT)	https://standards.ieee.org/develop/project/2413.html
Arrowhead Framework	www.arrowhead.eu

Ilustración 5: Iniciativas Arquitectura de referencia

No obstante vamos a reducir el modelo de IoT a las siguientes tres capas:

- El hardware de los dispositivos (sensores y actuadores).
- La infraestructura de comunicaciones.
- Las aplicaciones.

3. Dispositivos utilizados en IoT.

Sensores y actuadores [9] son piezas fundamentales para IoT. Posibilitan que objetos de la vida cotidiana interactúen entre ellos y los seres humanos a través de Internet o redes dedicadas, recopilando información del entorno o interactuado con él. Estos dispositivos son cada vez de menor tamaño, facilitando su integración en cualquier objeto.

La tendencia de estos dispositivos es la miniaturización y la creación de redes inteligentes de elementos simples. La nanotecnología junto a la miniaturización permite que el tamaño de los dispositivos sea mínimo sin disminuir su velocidad de funcionamiento y capacidad. Junto a la miniaturización, la separación del proceso en elementos hardware con capacidades limitadas, que cuando actúen en conjunto puedan conseguir grandes cosas, de manera que cada elemento se comunique con los otros elementos a su alrededor mediante lenguajes muy básicos.

IoT utiliza dispositivos electrónicos capaces de medir magnitudes físicas o químicas y transformarlas en señales eléctricas (sensores). Por otro lado también utiliza dispositivos capaces de utilizar señales eléctricas para activar un determinado proceso (actuadores). Estos dos tipos de dispositivos combinados con la capacidad de conexión forman la capa de hardware de IoT.

3.1. Sensores.

La información recogida por los sensores es convertida al mundo digital para poder así tratarla, almacenarla y enviarla a otros dispositivos. Los sensores pueden clasificarse de acuerdo a la magnitud vayan a leer en:

3.1.2. Físicos.

Transforman una magnitud física en información. Entran dentro de esta clasificación los sensores de temperatura, de presión, acelerómetros, galgas extensiométricas, sensores de lux giróscopos, inclinómetros,…

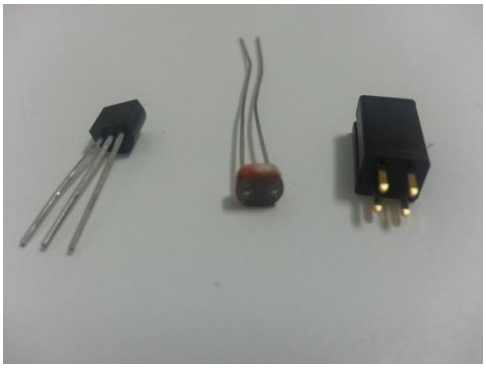


Ilustración 6: De izquierda a derecha: sensor de temperatura tmp36, ldr, sensor de inclinación

3.1.3. Químicos y bioquímicos.

Los sensores químicos miden concentraciones de distintos elementos o moléculas, proporcionando lecturas de la concentración de los elementos o moléculas medidas respecto del entorno. Estos sensores no permiten una operativa sencilla que se aplique fácilmente fuera de los laboratorios.

Los sensores bioquímicos pueden medir la concentración concreta de una proteica, acido nucleíco,…

La salida que proporcionan estos sensores es una señal analógica proporcional a la medida, que debe de ser convenientemente adaptada mediante un circuito.

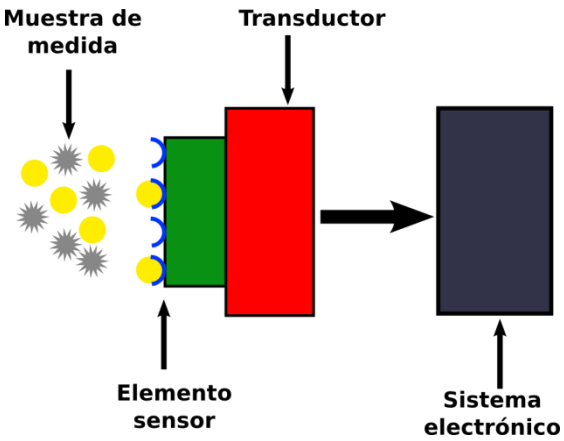


Ilustración 7: Esquema sensor bioquímico

3.2. Actuadores.

No están tan implantados como los sensores y a diferencia de éstos, los actuadores, a partir de una información digital, actúan en el mundo real.

3.2.1. Motores.

Dentro de los actuadores, los de uso más común, son los motores, existen múltiples tipos y formas diferentes de controlarlos.

Habitualmente estos se controlan utilizando modulación por ancho de pulso (PWM). Se envían pulsos de ancho variable para que el motor gire de forma proporcional a la anchura del pulso.

3.2.2. Servomotores

Este tipo de actuadores permite controlar la posición dentro de un rango y mantener fija esta posición. El control se realiza igualmente mediante señales PWM, siendo la duración de los pulsos la que indica la posición o el ángulo de rotación. Si no se envía señal alguna, el servo queda libre.

Ilustración 8: Servomotores.

3.2.3. Motores paso a paso (Steppers)

Son motores que pueden avanzar un determinado número de grados o pasos (steps) respecto de su eje. Se necesita un circuito y generar señales que se envían al motor, logrando pasos de pocos grados.

Ilustración 9: Motor paso a paso.

3.2.4. Electroválvulas.

Válvulas controladas electrónicamente que permiten o impiden el paso de líquidos o gases. Disponen de dos posiciones, abierto o cerrado, por lo que el control es sumamente sencillo.

Ilustración 10: Electroválvulas de vacío de 2 vías, de accionamiento directo.

3.3. Teléfonos móviles (smartphones)

No podemos dejar pasar los teléfonos móviles, ya que en sí mismos pueden ser sensores y actuadores. Además de permitir recibir llamadas y realizarlas, entre otras muchas más funcionalidades, disponen de múltiples sensores y actuadores:

- Acelerómetro: permite medir movimientos y conocer la posición del móvil.
- Magnetómetro: mide el campo magnético de la tierra.
- Giróscopo: mide movimientos, el ángulo y la velocidad de giro en las tres coordenadas espaciales.

- Sensores de iluminación: registra la cantidad de luz ambiental.
- Sensores de temperatura: temperatura ambiental limitada a un rango de valores habituales (-20º a 50º).
- Sensores acústicos: Están equipados con micrófonos que permiten registrar el sonido.
- Barómetro: mide la presión atmosférica.
- Sensor táctil: recibe entradas múltiples simultáneamente.
- GPS: Proporciona la posición en coordenadas espaciales y la velocidad a la que se mueve el dispositivo, con precisiones de pocos metros y Km/h.

4. Protocolos de comunicaciones.

IoT está creciendo rápidamente, existen una gran cantidad de dispositivos conectados a internet, y su número aumenta exponencialmente. Estos dispositivos están equipados con baterías, un mínimo de almacenamiento y capacidad de proceso. Debido a estas restricciones, la comunicación entre estos dispositivos acarrea varios desafíos:

1. Direccionamiento e identificación.
2. Comunicaciones con bajo consumo de energía.
3. Protocolos de enrutamiento eficientes y bajos requerimientos de memoria.
4. Alta velocidad y comunicaciones sin pérdida.
5. Movilidad.

Los dispositivos IoT, generalmente se conectan a Internet a través de la pila TCP/IP, esta pila es muy compleja y necesita gran cantidad de memoria y energía. También pueden conectarse localmente a través de redes no IP, en la que el consumo de energía es menor y conectarse a internet a través de una pasarela (Gateway). Algunas redes no IP, como Bluetooth, RFID y NFC son muy populares pero con un alcance reducido, por lo que las aplicaciones están limitadas a redes PAN (personal área network). Para aumentar el alcance, es necesario modificar la pila TCP/IP con el objetivo de reducir el consumo de energía.

Las organizaciones de desarrollo de estándares (standards development organizations, SDO) definen una visión común de la arquitectura, protocolos y funcionalidad. Los protocolos de comunicación se pueden clasificar en función del rango o consumo de los dispositivos en: sistemas M2M capilares y sistemas M2M celulares.

M2M (machine to machine), hace referencia al intercambio de datos entre dos máquinas conectadas entre sí, a través de un enlace directo o a través de una red, para enviar y recibir datos.

Las regulaciones del espectro radioeléctrico no permiten el uso de todo el espectro, lo clasifican en distintas bandas para regular su uso, dejando algunas para uso libre de acuerdo a unas normas. Estas son las llamadas ISM (industrial, scientific and medical).

Suelen ser las de 433 MHz, 868 MHz o 905 MHz y la de 2,4 GHz. Por encima de esta última hay mas bandas libres (5 GHz para WIMAX, Wi-Fi con especificación 802.11a, n, y ac). También existen bandas de frecuencias por debajo de 433 MHz, pero no son de uso común en IoT.

En el mercado existen diferentes sistemas de comunicación inalámbricos que cubren todos los aspectos de la comunicación, en unos casos, y en otros, diferentes soluciones proporcionan una solución completa.

No obstante, todas o la práctica totalidad, utilizan un modelo de red común, el modelo OSI (open system interconect).

4.1. Modelo OSI

El modelo de interconexión de sistemas abiertos (OSI), es un modelo de red creado por la Organización Internacional de Normalización. Se consideran siete niveles, en cada uno de ellos se procesan unidades de información denominadas PDU (Unidad de datos de protocolo). En los dispositivos emisores las PDU se transmiten del nivel superior al inferior, y en cada uno de ellos se añade información de control (cabeceras, **A**pplication**H**eader, **P**resentation**H**, **S**ession**H**, **T**ransport**H**, **N**etwork**H**, Datalink**H**, o terminales DT, correspondientes a cada uno de los niveles). En los dispositivos receptores la información se procesa desde el nivel inferior, comprobando y eliminando en cada nivel las cabeceras o terminales de cada PDU correspondiente a dicho nivel.

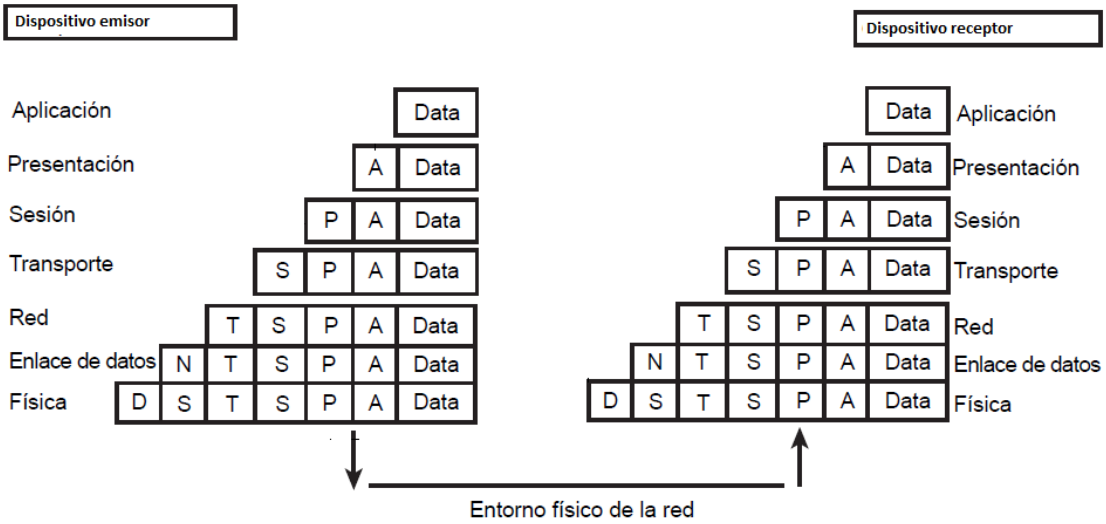


Ilustración 11: Los datos bajan por la pila OSI del dispositivo emisor y suben por los del dispositivo receptor

Una vez visto el modelo teórico que determina como la información viaja de un dispositivo a otro dentro de una red, vamos a pasar a explicar algunos de los protocolos utilizados por IoT, equiparándolos con las capas del modelo OSI. Así tendremos una visión clara y sencilla del modo en que operan estos protocolos, la forma en que transportan los datos y una taxonomía de los mismos dentro de cada una de las capas del modelo, atendiendo a la clasificación anteriormente citada.

4.2. Sistemas M2M capilares

Una red capilar (Capillary network) es una red de área local que utiliza tecnologías de radioacceso de corto alcance para proporcionar conectividad a grupos de dispositivos. Aprovechan las capacidades clave de las redes celulares: la ubicuidad, seguridad integrada, gestión de redes y conectividad de backhaul (redes de retorno) avanzada. Generalmente utilizan topologías en estrella, en la que todos los dispositivos se comunican con un nodo central o malladas, donde todos dispositivos pueden conectarse con todos los demás, bien directamente o usando nodos intermedios.

4.2.1. Capa física y enlace.

En la capa física es donde se especifican los parámetros mecánicos (grosor de los cables, tipo de conectores), eléctricos (temporizador de las señales, niveles de tensión) de las conexiones físicas.

Las unidades de información que consideran son bits, y trata de la transmisión de cadenas de bits en el canal de comunicación (pares trenzados de cobre, cable coaxial, radio, infrarrojos, fibra óptica), si el emisor envía un 0, al receptor debe de llegar un 0.

La capa de enlace define la conexión segura entre dos dispositivo, de manera que no se pierdan datos, y en el caso de múltiples dispositivos compartiendo el mismo medio, es un modo de arbitrar quién puede usar el medio en cada momento. Lo realiza descomponiendo los mensajes que recibe del nivel superior en tramas o bloques de información, en las que añade una cabecera (DH) e información redundante para control de errores. La cabecera suele contener información de direcciones de origen y destino, ruta que va a seguir la trama, etc… también se encarga de transmitir sin error las tramas entre cada enlace que conecte directamente dos puntos físicos (nodos) adyacentes de la red, y desconectar el enlace de datos sin pérdidas de información.

A continuación se muestran las distintas tecnologías que se agrupan dentro de estas capas. Algunas de las tecnologías presentadas, especifican varias capas del modelo OSI, se presentan en los niveles mas bajos del modelo aunque tengan presencia en otros niveles superiores.

4.2.1.1. IEEE 802.15.1 (Bluetooth)

Bluetooth es una especificación de la industria para la conectividad basada en radio frecuencia (RF) de corto alcance para dispositivos personales portátiles. Diseñada inicialmente para un corto alcance y tasas de transferencia medias (hasta 1Mbps) en la frecuencia de 2,4 GHz.

En 2011 aparece Bluetooth Low Energy (BLE o LE), que como indica su nombre reduce el consumo de energía. Con BLE, los dispositivos pueden utilizar baterías que pueden durar años, aspecto vital para aplicaciones que solo necesitan intercambiar pequeñas cantidades de datos periódicamente.

Al igual que Bluetooth, BLE opera en la banda libre de 2,4 GHZ, pero a diferencia de este, permanece en espera hasta que se necesita transmitir datos.

4.2.1.2. RFID

Los sistemas de identificación por radiofrecuencia o RFID (Radio Frequency Identification) son una tecnología para la identificación de objetos a distancia sin necesidad de contacto. Es necesario una etiqueta o tag RFID, esta consiste en un microchip que va adjunto a una antena de radio y que va a permitir la identificación unívoca del elemento portador de la etiqueta.

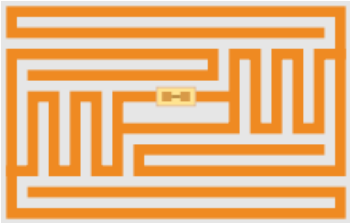


Ilustración 12: Etiqueta RFID

Las bandas de frecuencia en las que trabajan los sistemas RFID son 125 o 134 KHz. para baja frecuencia y 13’56 MHz para alta frecuencia, aunque pueden trabajar en muchos otros rangos de frecuencia. Para el uso del espectro UHF los distintos países no consiguen llegar a un estándar ya que en Europa se trabaja en 868 MHz, en Estados Unidos 915 MHz y en Japón, reticentes al uso de esta banda, empiezan a trabajar en 960 MHz. El problema que se genera en el empleo de la banda UHF es que hay distintos dispositivos que operan sobre la misma, y generan ruidos sobre los sistemas RFID y viceversa, con lo cual los gobiernos tienen que realizar detallados estudios para determinar y minimizar los trastornos que puedan suceder como consecuencia de cambiar las bandas de trabajo de los dispositivos RFID.

4.2.1.3. Near Field Communication (NFC)

Es una tecnología de comunicación inalámbrica de muy corto alcance, a través de la cual los dispositivos móviles pueden interactuar entre sí a una distancia de pocos centímetros. NFC se basa en RFID, utiliza variaciones en el campo magnético para la transmisión de datos y opera en la banda de 13,56 MHz Posee dos modos de operación: activo y pasivo. En el modo activo, ambos dispositivos generan campos magnéticos, mientras que en el modo pasivo solo un dispositivo los genera. A diferencia de RFID, NFC puede ser utilizado para comunicación en dos sentidos.

4.2.1.4. IEEE 802.11 (Wi-Fi) & 802.11 Low Power

Los estándares IEEE 802.11 (Wi-Fi) utilizan las bandas de 2,4 GHz, 5 GHz y 60 GHz para tener una tasa de transferencia del orden de decenas o cientos de Mbps, con un alcance moderado a costa de un consumo elevado. Existen varias revisiones o propuestas del estándar: 802.11a, 802.11b, 802.11g, etc. habitualmente incompatibles entre ellas.

En el 2016 la Wi-Fi Alliance anunció la salida de Wi-Fi HaLow para productos que incorporan tecnología IEEE 802.11ah. HaLow opera en bandas de frecuencias inferiores a 1 GHz, permitiendo una gama más amplia de conectividad de menor potencia que los productos Wi-Fi Certified. De esta manera HaLoW permitirá una gran variedad de casos de uso eficiente de energía, como pueden ser el hogar inteligente, coche y salud digital, la industria, agricultura y entornos de Smart City.

HaLow amplia Wi-Fi en la banda de los 900 MHz, con conectividad de baja potencia para aplicaciones y sensores portátiles. El alcance es casi el doble que el de la Wi-Fi de hoy, y no sólo será capaz de de transmitir mas señales, sino que también permitirá conexiones mas robustas en

entornos hostiles donde la capacidad de penetrar en paredes y otras barreras es importante. HaLow adoptará los protocolos Wi-Fi existentes y ofrecerá numerosas ventajas a los consumidores.

4.2.1.5. Z-Wave

Se trata de una tecnología de comunicación basada en RF, diseñada específicamente para controlar, monitorizar y comprobar el estado de aplicaciones en entornos residenciales y comerciales. Se trata de una tecnología madura, ampliamente probada y desplegada.

Z-Wave permite transmisiones seguras, de baja latencia y bajas tasas de velocidad, de pequeños paquetes de datos, de hasta 100kbits/s. Está destinado para aplicaciones que utilizan sensores y actuadores. A diferencia de Wi-Fi y otras redes IEEE 802.11, en este protocolo los dispositivos mantienen una distancia máxima de unos cien metros, de manera que los mensajes de un dispositivo pueden saltar entre varios hasta llegar al concentrador o controlador de la casa.

La industria domótica ha acogido rápidamente este estándar debido a su simplicidad, pudiéndose encontrar en el mercado multitud de dispositivos compatibles.

Entre las características principales podemos citar:

- Tecnología de comunicaciones de baja potencia basada en RF que soporta redes malladas sin necesidad de nodos coordinadores.
- Opera en la banda de 868 MHz y es impermeable a la interferencia de Wi-Fi y otras tecnologías inalámbricas en el rango de 2,4 GHz (Bluetooth, ZigBee, etc.).
- Los niveles PHY y MAC están definidos por la recomendación ITU-T G9959.
- Diseñado para el control y estado de aplicaciones soporta tasas de transferencia de hasta 100kbps con encriptado AES128, IPV6 y operación multicanal.

4.2.1.6. IEEE 802.15.4

Es un estándar que define el nivel físico y el control de acceso de las redes de corto alcance WPAN (Wireless personal area networks). Estas redes se caracterizan por su bajo costo y baja velocidad entre dispositivos, a diferencia de otros enfoques como WiFi, que permiten mayor ancho de banda a costa de de requerir mayor potencia. El objetivo del estándar la comunicación a muy bajo costo de dispositivos cercanos con poca o ninguna infraestructura subyacente para reducir el consumo de energía aun mas. El estándar básico contempla un alcance de 10 m, con una velocidad de transferencia de 250 kbit/s.

El estándar incluye, compatibilidad en tiempo real por reserva de ranuras de tiempo garantizadas, evitar colisiones a través de CSMA / CA y soporte integrado para comunicaciones seguras. Los dispositivos también incluyen funciones de administración de energía, tales como calidad de enlace y detección de energía.

IEEE 802.15.4 puede utilizar una de las tres posibles bandas de frecuencia para el funcionamiento (868/915/2450 MHz). Las especificaciones establecidas por el estándar son la base para estándares más complejos, como ZigBee, ISA100.11a, WirelessHart, Open-WSN, etc.

	ZigBee	WirelessHart
Aplicación	Aplicaciones y seguridad	Comandos, tipos de datos predefinidos, aplicaciones
Presentación		
Sesión		
Transporte		Transferencia auto segmentada de grandes conjuntos de datos, transporte seguro y tamaños de segmento negociados
Red	Red mallada con enrutamiento ad hoc	Consumo optimizado de energía, red mallada de rutas redundantes.
Enlace de datos	IEEE 802.15.4	IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH)
Físico	IEEE 802.15.4	IEEE 802.15.4 2,4 GHZ

Ilustración 13: ZigBee WirelessHart y OSI

4.2.1.7. WirelessHART

Es una tecnología WSN (wireless sensor network) que se basa en el protocolo HART (Highway Addressable Remote Transducer). El estándar se definió para satisfacer los requisitos de de los dispositivos de las redes de sensores. Esta tecnología está diseñada para ser una red de dispositivos tipo mesh, que se auto-organiza y se auto-repara.

Opera en la banda ISM de 2,4 GHz utilizando IEEE 802.15.4. En una red WirelessHART, cada estación o dispositivo de campo establece una red, actuando simultáneamente como fuente de señal y como repetidor. El transmisor original envía un mensaje al dispositivo más cercano, el cual pasa el mensaje hacia otros dispositivos, hasta que el mensaje alcanza la estación base y su destinatario.

Pueden configurarse rutas alternativas la inicialización, de modo que si el mensaje no puede ser transmitido por una ruta se pasa automáticamente a una ruta alternativa. Además de aumentar el rango de la red, se proveen rutas de comunicación redundantes para aumentar la confiabilidad.

WirelessHART incorpora saltos de canal (frequency hopping) para evitar interferencias, de acuerdo a normas como IEEE 802.15.4, DSSS (espectro ensanchado por secuencia directa o direct sequence spread spectrum), y CSS (Chirp spread spectrum). Esto permite operar, incluso en presencia de otras redes en la banda de los 2.4 GHz. Posee mecanismos de seguridad, como encriptación AES1128, gestión de código, y autenticación, para proteger la red.

	ZigBee	Z-Wave	6LowPAN	WirelessHART	Bluetooth	WiFi	NFC	RFID
Frecuencia de operación	2,4 GHz, 915 MHz, 868 MHz	900 MHz	2,4 GHz	2,4 GHz	2,4GHz	2,4 GHz, 5 GHz	13,56 MHz	LF:125-134KHZ HF:13,56MHz UHF:856-960MHz
Alcance	500 m	100 m	200 m	250 m	50 m	100 m	10cm	10cm,30cm,100m
Tasa de datos	250 Kbps	40 Kbps	200 Kbps	250 Kbps	1 Mbps	600 Mbps	424Kbps	424 kbps
Número de nodos	65.536	232	100	30.000	8	N/A	2	N/A
Consumo medio	Tx:25-30mA Rx:20-30mA	Tx:30-40mA Rx:20-30mA	Tx:20-35mA Rx:12-25mA	Tx:18-25mA Rx:6-10mA	Tx:15-20mA Rx:15-20mA	Tx: >220mA Rx:>215mA	Bajo con baterias	Depende del modelo de etiqueta
Interoperabilidad	Alta	Alta	Baja	Alta	Media	alta	alta	alta

Ilustración 14: Comparación de protocolos

4.2.1.8. Especificaciones LPWA.

En este subapartado recogemos las especificaciones de las LPWA (low power wide area networks), que se caracterizan por:

- Conectar dispositivos de bajo consumo, equipados con baterías con duración de varios años.
- Conectar dispositivos con bajos requerimientos de ancho de banda.
- Operar a grandes distancias.

Existen multitud de especificaciones, la mayor parte propietarias, que abarcan los siete niveles OSI. En el caso de Lora especifica el nivel físico y LoraWan el nivel de enlace de datos, mientras que SigFox, especifica, del nivel físico al nivel de transporte:

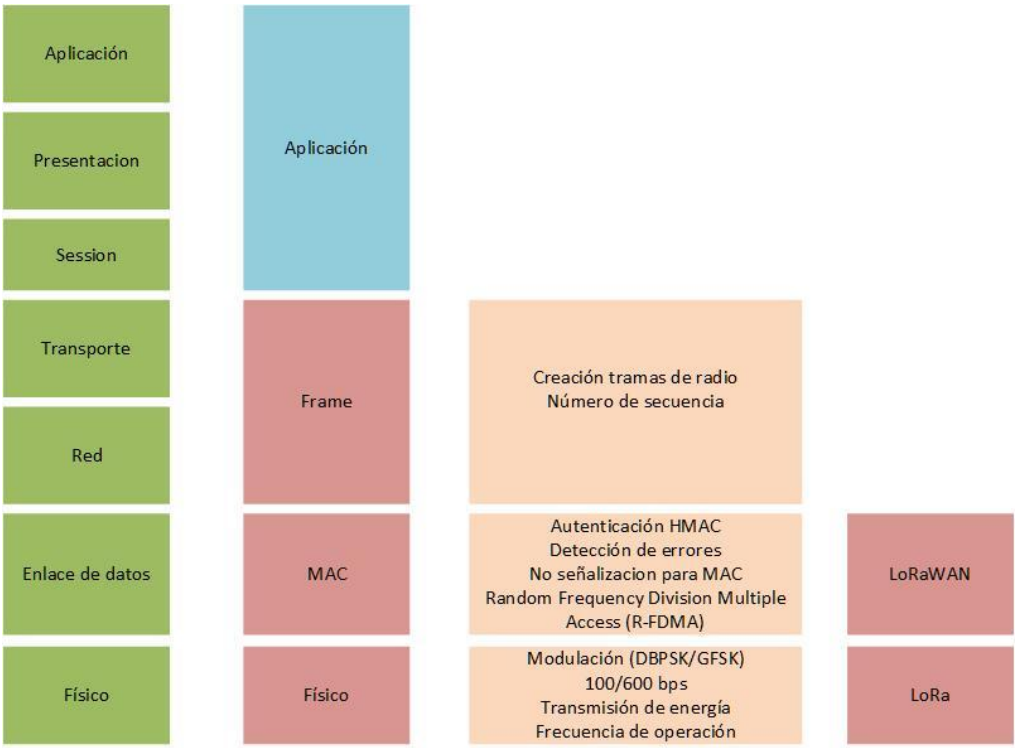


Ilustración 15: OSI vs Sigfox vs Lora

Dedicaremos, mas adelante un apartado especifico para estas tecnologías.

4.2.2. Capa de red.

Las funciones que realiza la capa de red son las siguientes:

- Se encarga de Fragmentar los segmentos que se transmiten entre dos equipos de datos en unidades denominadas paquetes. En el ordenador receptor se efectúa el proceso inverso: los paquetes se ensamblan en segmentos.
- Realiza el encaminamiento de los paquetes. Utiliza algoritmos eficientes para la elección de la ruta más adecuada en cada momento, para remitir los paquetes a cada uno de los nodos de la red que estos deban atravesar para llegar a su destino.
- Previene la producción de bloqueos así como la congestión en los nodos de la red de transporte que pudiesen producirse en horas punta por la llegada de paquetes en forma masiva.

IP y especialmente IPv6, están diseñados para el Internet de hoy día con ordenadores personales, portátiles y servidores conectados por cable. No obstante las restricciones de los dispositivos de los sistemas de IoT, hacen que las características de los protocolos actuales no se adecuen a las necesidades especificas de estos dispositivos, por lo que es necesario el desarrollo de nuevos o adaptación de los existentes.
A continuación se muestran las especificaciones de más alto nivel, basadas en las capas anteriores, que en la actualidad, tienen una mayor frecuencia de uso.

4.2.2.1. IETF 6LoWPAN

6LoWPAN es el acrónimo de IPv6 over Low power Wireless Personal Area Networks, es decir, la adaptación del protocolo IP versión 6 a redes de bajo consumo tipo IEEE 802.15.4 y sus diferentes características. El objetivo final de este estándar es proveer de una dirección IP (versión 6) a todo dispositivo inalámbrico, pudiendo así direccionarse y accederse directamente.

Las WPAN sobre las que se producen muchas de las comunicaciones de IoT, poseen características especiales que las diferencian de otras tecnologías de la capa de enlace. Una de estas es el tamaño del paquete, limitado a 127 bytes para IEEE 802.15.4, diferentes longitudes y bajo ancho de banda. Fue necesario implementar una capa de adaptación que se ajustara a los paquetes IPV6 a la especificación IEEE 802.15.4. El IETF 6LoWPAN desarrolló este estándar en 2007 que especifica los servicios de mapeo que necesita IPv6 sobre WPANs de baja potencia. El estándar proporciona una compresión de encabezado para reducir la sobrecarga de la transmisión, la fragmentación para cumplir con el requerimiento de la MTU (maximun transfer unit) de IPv6 y el reenvío de la capa de enlace para soportar múltiples saltos. Los datagramas envueltos por 6LoWPAN son acompañados por una combinación de encabezados. Estos encabezados pueden ser de cuatro tipos, identificados por dos bits:

- 00-NO 6LoWPAN header. El encabezado NO 6LoWPAN, hace que los paquetes que no se ajusten a la especificación sean descartados.
- 01-Dispatch headr. La compresión de encabezados IPv6 o multidifusión, se realiza mediante el encabezado Dispatch.
- 10-Mesh addressing. El encabezado Mesh addressing, identifica los paquetes IEEE 802.15.4 que tienen que ser reenviados a la capa de enlace.
- 11-Fragmentation. El encabezado Fragmentation, se utiliza en datagramas cuyas longitudes exceden una trama IEEE 802.15.4.

6LoWPAN elimina muchos problemas, de manera que un pequeño datagrama IPv6 puede ser enviado a través de un único salto IEEE 802.15.4 en el mejor de los casos. También puede comprimir los encabezados IPv6 a 2 bytes

	6LoWPAN		Low-power Wi-Fi	
Packet size	8 Bytes	1024 Bytes	8 Bytes	1024 Bytes
Time (ms)	6	23.61	11.3	16.58
Energy (mJ)	2.5	9.17	0.55	1.28

10x

Ilustración 16: Comparativa 6LoWPAN y Low-power Wi-Fi

4.2.2.2. ZigBee

Se trata de otra especificación de alto nivel para redes tipo IEEE 802.15.4. Especifica todas las capas de protocolo capa de red (para enrutado), capa de aplicación, especificación de dispositivos (ZDO o ZigBee device objects) y objetos de aplicación, partiendo de las capas física y de acceso al medio (MAC) de IEEE 802.15.4,

ZigBee ha sido diseñado para satisfacer la necesidad de crear redes de baja potencia que cubran grandes áreas. La gran mayoría de los dispositivos ZigBee están alimentados por baterías, por lo que el consumo de energía es un factor crítico. Los dispositivos ZigBee permiten la construcción de redes de nodos malladas.

La distancia entre dispositivos adyacentes puede llegar a 10 metros en aplicaciones de mínimo consumo de energía, opera en la banda de 2,4 GHz y en la de 915 MHZ o la de 868 MHZ, con una tasa de transferencia de 255 kbps en 2,4 GHz y a tasas menores y bandas inferiores al GHz. Permite el encriptado AES-128 y una gran variedad de métodos de distribución de claves. La redes ZigBee pueden estar compuestas por miles de nodos, los mensajes se pasan de un nodo a otro a través de la red y no hay necesidad de que ningún nodo individual esté dentro del alcance de transmisión de todos los miembros de la red, pudiendo los nodos formar redes de con topología en estrella o mallada. Así la pérdida de un nodo no interrumpirá el funcionamiento de la red.

Pueden colocarse enrutadores ZigBee para extender la red donde los nodos finales están demasiado separados para comunicarse con los nodos vecinos.

La ZigBee Alliance, fundada en 2002, mantiene y actualiza los estándares, está compuesta por varios cientos de compañías y fabricantes como Texas Instruments, Cisco y Huawei.

4.2.3. Capa de transporte.

Se encarga del transporte de la información, desde la fuente al destino, a través de la red, sin pérdidas.

Los accesos a la capa de transporte se efectúan a través de puertos (sockets). EL objetivo es realizar un servicio de transporte eficiente entre procesos o usuarios finales. Para dicho fin, toma los mensajes del nivel de sesión, los distribuye en pequeñas unidades (Segmentos) y los pasa a la red. Los protocolos de la capa de transporte se aseguran que todos los segmentos lleguen de forma correcta a su destino, para lo cual realizan detección y corrección de errores, además de controlar el flujo y la secuenciación.

El nivel de transporte proporciona control de congestión y entrega segura de paquetes, que dentro de la arquitectura TCP/IP se consigue con TCP (transport control protocol) protocolo de transporte dominante en Internet.

Sin embargo, el modelo de comunicación orientado a flujos de bytes de TCP, no resulta óptimo para aplicaciones IoT, donde los dispositivos, para ahorrar batería, se desconectan, por lo que no es posible mantener conexiones de larga duración. Las comunicaciones IoT suponen la transmisión de pequeñas cantidades de datos, que hacen que el establecimiento de la conexión para cada una de esas transferencias una sobrecarga, que se traduce en un mayor consumo de energía. Por último, los propios mecanismos que TCP proporciona para la entrega segura de paquetes, puede introducir retardos que impidan que dispositivos como los actuadores no lleven a cabo, de forma eficiente, su cometido, el tamaño de la cabecera limita su aplicación en redes como 802.15.4 donde el MTU a nivel de MAC es de 127 bytes. En esos casos tenemos UDP, bastante más simple en cuanto a implementación y tamaño de la cabecera.

El protocolo de datagramas de usuario (UDP) es un protocolo de capa de transporte d. Proporciona un servicio de datagramas de mejor esfuerzo (best-effor). UDP no proporciona ninguna garantía de entrega y no hay protección contra la duplicación de datagramas, pero su simplicidad reduce la sobrecarga del protocolo y puede ser adecuado para algunas aplicaciones en lugar de TCP.

Un dispositivo puede enviar paquetes UDP sin necesidad de establecer primero una conexión con el destinatario. El dispositivo completa los campos del encabezado UDP y lo envía junto con los datos para su transmisión por la capa de red IP.

Generalmente UDP es apropiado en aplicaciones donde la velocidad es más crítica que la confiabilidad. Por ejemplo, utilizar UDP en una

aplicación que envía datos desde un punto de adquisición rápido donde es aceptable perder algunas medidas.

4.2.4. Capa de sesión, presentación y aplicación.

La capa de sesión es responsable de:

- Actuar de interfaz entre el usuario y la red, gestionando el establecimiento de la conexión entre procesos remotos.
- Establecer un dialogo entre dos equipos remotos para controlar la forma en que se intercambian los datos.
- Identificar los usuarios de procesos remotos
- Cuando se corta la conexión de forma anormal, en la capa de transporte o en inferiores, la capa de sesión puede encargarse de restablecer la sesión de forma transparente al usuario.

Su función es aumentar la fiabilidad de la comunicación obtenible por las capas inferiores, proporcionando el control de la comunicación entre aplicaciones al establecer, gestionar y cerrar sesiones o conexiones entre las aplicaciones que se comunican.

La capa de presentación trata de homogeneizar los formatos de representación de los datos entre equipos de la red.

Para homogeneizar la representación de datos (Textos, Sonidos, imágenes, valores numéricos, instrucciones), la capa de presentación interpreta las estructuras de las informaciones intercambiadas por los procesos de la aplicación y las transforma convenientemente.

Puede realizar transformaciones para conseguir mayor eficacia en la red (compresión de texto y cifrado de seguridad). Los programas del nivel 6 suelen incluirse en el propio Sistema Operativo.

La representación de los caracteres como los datos de texto y numéricos dependen del Ordenador, se representan por códigos de representación EBCDIC, ASCII y UNICODE.

La capad de aplicación permite que los dispositivos se intercomuniquen a través de procesos, estos se corresponden con unas determinadas aplicaciones. El intercambio de información entre dos procesos se efectúa por medio de algún protocolo de la capa de aplicación.

En estas capas se han propuesto muchos protocolos para IoT para facilitar y simplificar la programación de aplicaciones, a los programadores y proveedores de servicios. Existen diferentes grupos que proporcionan protocolos para IoT, entre los que se incluye el World Wide Web Consortium (W3C), el Internet Engineering Task Force (IETF), EPCglobal, Institute of Electrical and Electronics Engineers (IEEE) y European Telecommunications Standards Institute (ETSI).

4.2.4.1. HTTP

Es un protocolo de comunicación del nivel de aplicación, que permite las transferencias de información en la Web. Desarrollado por el W3C y el IETF. Sigue el paradigma cliente-servidor, el cliente realiza peticiones a un servidor que sirve las peticiones a los clientes.

Las peticiones se realizan mediante mensajes HTTP (HyperText Transfer Protocol), estos se envían sobre texto plano lo que hace que los mensajes sean largos, característica que junto a otras en las que se basa su diseño, hacen que su uso no sea óptimo para redes de comunicación de bajo consumo.

4.2.4.2. CoAP.

El uso de servicios web en Internet se ha generalizado en la mayoría de las aplicaciones, y estos servicios web dependen de REST (REpresentational State Transfer).

El grupo de trabajo IETF Constrained RESTful Environments (CoRE) tiene como objetivo crear una arquitectura REST adecuada para dispositivos limitados. Las redes de dispositivos limitados como 6LoWPAN se basan en la fragmentación de los paquetes IPv6 en unidades más pequeñas del nivel de enlace, sin embargo, esto causa una reducción significativa en la probabilidad de entrega. CoAP [10] se diseña para mantener una sobrecarga de mensajes baja, limitando así la necesidad de fragmentación.

Una de las principales metas de CoAP es diseñar un protocolo web genérico para los requisitos especiales de entornos restringidos, considerando especialmente las necesidades energéticas, automatización de edificios y otras aplicaciones M2M. El objetivo de CoAP no es comprimir ciegamente HTTP, sino realizar un subconjunto de REST (REpresentational State Transfer).

CoAP define un protocolo de transferencia web que se basa en la representación del estado de la transferencia encima de las funcionalidades HTTP.

REST representa una forma simple de intercambiar datos entre clientes y servidores sobre HTTP, puede verse como un protocolo de conexión que depende de la arquitectura cliente-servidor. Se usa en aplicaciones móviles y de redes sociales y elimina la ambigüedad utilizando los métodos HTTP, get, post y delete. REST permite a los cliented y servidores publicar y consumir servicios web como SOAP (Simple Object Access Protocol) de forma simple, utilizando Unifor Resource Identifiers (URIs) como nombres y los métodos HTTP get, post, put y delete como verbos.

- GET: Solicita la obtención de un recurso concreto. Una GET obtiene los datos solicitados sin afectar a los datos.
- PUT: Solicita guardar los datos transmitidos en un recurso concreto. Si el recurso ya existe, se modifica, en caso contrario se crea.
- POST: Solicita almacenar los datos transmitidos, no se especifica en qué recurso se deben almacenar.
- DELETE: Elimina el recurso especificado.

No necesita XML para el intercambio de mensajes, como lo hace REST. A diferencia de HTTP, CoAP utiliza UDP para el intercambio de

mensajes asíncronamente, que lo hace más adecuado para las aplicaciones IoT. CoAP modifica algunas funcionalidades HTTP para cumplir con las necesidades IoT (bajo consumo y funcionamiento en entornos ruidosos). Sin embargo, debido a que CoAP ha sido diseñado basándose en REST, la conversión entre estos dos protocolos en los proxies REST-CoAP es sencilla.

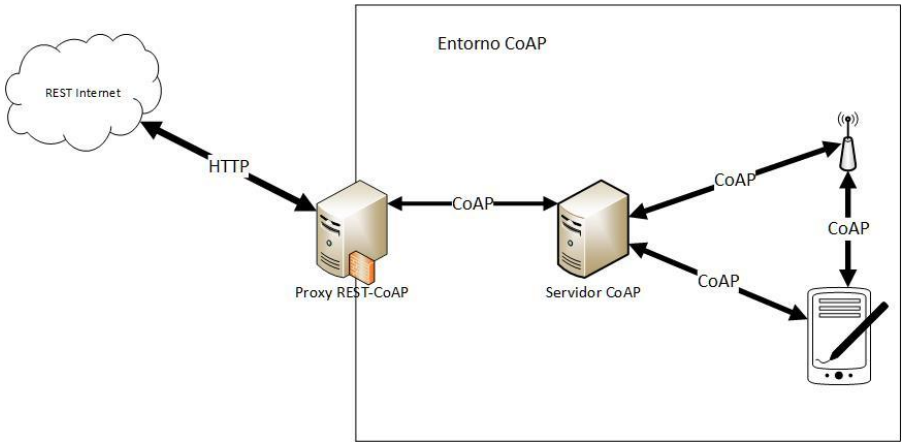


Ilustración 17: Entorno CoAP

CoAP permite a pequeños dispositivos de bajo consumo, capacidad de proceso y de comunicación y utilizar las interacciones RESTful. Puede ser dividido en dos subniveles: mensaje y petición/respuesta.

El nivel de mensaje detecta duplicidades y proporciona comunicaciones seguras sobre UDP utilizando retroceso exponencial ya que UDP no posee ningún mecanismo de recuperación de errores.

El Nivel petición/respuesta utiliza comunicaciones REST. CoAP utiliza cuatro tipos de mensajes: confirmable, non-confirmable, reset y acknowledgement.

- Confirmable message: algunos mensajes necesitan confirmación (ACK) Estos se denominan “confirmable”. Cuando no hay pérdida de paquetes, cada mensaje confirmable, produce exactamente un mensaje de retorno de tipo ACK o reset.
- Non confirmable Message: Algunos mensajes no requieren ACK. Esto es particularmente cierto, para mensajes que se repiten regularmente, debido a necesidades de la aplicación.
- Mensaje reset: Un reset indica que un determinado mensaje (confirmable o non-confirmable) fue recibido, pero algo se perdió o no se ha procesado convenientemente.
- Mensaje de confirmación: Un mensaje de confirmación, confirma que un mensaje confirmable ha llegado. Un mensaje de confirmación no indica el acierto o fallo de ninguna petición encapsulada en el mensaje confirmable, sin embargo, la confirmación puede transportar una respuesta (piggybacked).

La fiabilidad se consigue con una mezcla de mensajes confirmable y non-confirmable que también emplea cuatro tipos diferentes de respuestas:

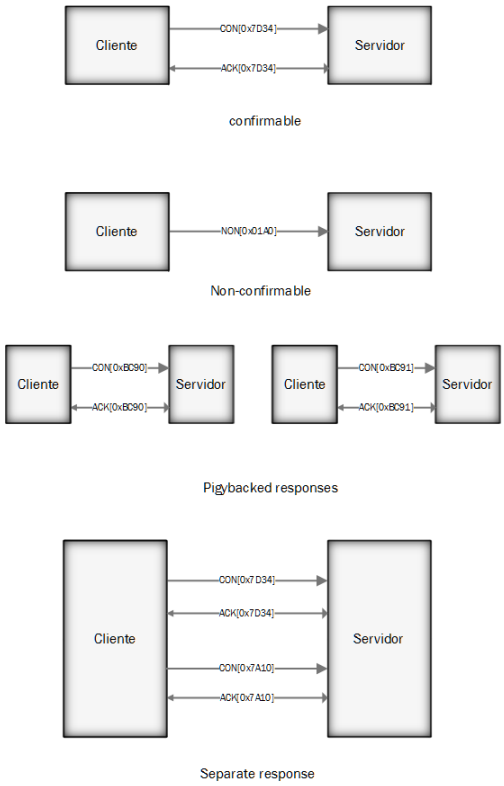


Ilustración 18: Tipos de respuestas

El modo de respuesta separada se utiliza cuando el servidor necesita esperar un tiempo antes de contestar al cliente. En el modo respuesta non-confirmable, el cliente envía datos sin esperar un mensaje ACK, utilizándo los IDs de los mensajes para detectar duplicados. En el lado del servidor se responde con un mensaje RST cuando se produce un problema de comunicación o se pierde un mensaje. Los mensajes confirmados suponen una aceptación ACK, si se pierden, estos se retransmiten un número limitado de veces. Los mensajes no confirmados se pueden emplear para aquellos casos en que es preferible perder la información periódica de algunos sensores, antes que saturar la red con retransmisiones, algo que no es posible con el modelo REST-HTTP.

CoAP presenta una API idéntica a REST-HTTP, es decir, el conjunto de operaciones CRUD (Create, Read, Update y Delete), por ejemplo, el método GET puede utilizarse para solicitar a un cliente la temperatura, si la temperatura está disponible, el cliente, entonces, la envía el correspondiente menaje ACK (piggybacked). En caso de no existir el dato, responde con un código de estado para indicar que los datos solicitados no se pueden encontrar. CoAP utiliza un formato simple para codificar mensajes. La primera parte y la parte fija de cada mensaje tienen cuatro bytes de encabezado. De esta manera un valor token puede aparecer con una longitud que varía de 0 a 8 bytes. El valor token se utiliza para correlacionar peticiones y respuestas. Un típico mensaje CoAP puede variar de 10 a 20 bytes.

Algunas de las características que aporta CoAP son:

- Suscripciones bajo demanda para monitorizar recursos de interés mediante publicación/suscripción.

- Transporte de recursos en forma de bloqueo: capacidad para intercambiar datos del transceptor entre el cliente y el servidor sin la necesidad de actualizar todos los datos para reducir sobrecarga en la comunicación.
- Descubrimiento de recursos: el servidor utiliza URI. Permite al cliente el descubrimiento de recursos.
- Interacción con HTTP: flexibilidad de comunicación con varios dispositivos debido a que la arquitectura REST permite interactuar fácilmente con HTTP a través de un proxy.
- Seguridad: CoAP es un protocolo seguro ya que está construido en la parte superior de DTLS (datagram transport layer security) para garantizar la integridad y confidencialidad de los mensajes.

4.2.4.3. Message Queue Telemetry Transport (MQTT)

MQTT [11] es un protocolo de mensajes introducido por Andy Standord-Clark de IBM y Arlen Nipper de Arcom (ahora Eurothech) en 1999, estandarizado mas tarde en 2013 por OASIS. El objetivo de MQTT es la conexión de dispositivos empotrados, la conexión utiliza un mecanismo de routing (uno a uno, uno a muchos, muchos a muchos) convirtiendo a MQTT un protocolo de conexión ideal para IoT y M2M. Utiliza publicación/suscripción para una transmisión flexible y una implementación simple, también se ajusta a dispositivos de recursos limitados que utilizan enlaces de bajo ancho de banda y o poco seguros. Está construido sobre TCP y permite la entrega mensajes a través de tres niveles de calidad de servicio (QoS).

Existen dos especificaciones principales para MQTT: MQTT v3.1 y MQTT-SN v1.2, también denominada MQTT-S. Esta última definida específicamente para redes de sensores, define un mapeo UDP de MQTT y añade soporte bróker. Este protocolo se basa en la transmisión de mensajes entre diferentes dispositivos con un elemento central, el broker, que es el que gestiona las comunicaciones de manera centralizada y garantiza que en la mayoría de los casos no haya pérdida de mensajes, hay múltiples implementaciones de brokers compatibles con el protocolo MQTT, algunos de los más populares son Mosquitto, ActiveMQ o RabbitMQ. La especificación proporciona tres elementos: conexión, semántica, enrutamiento y puntos finales.

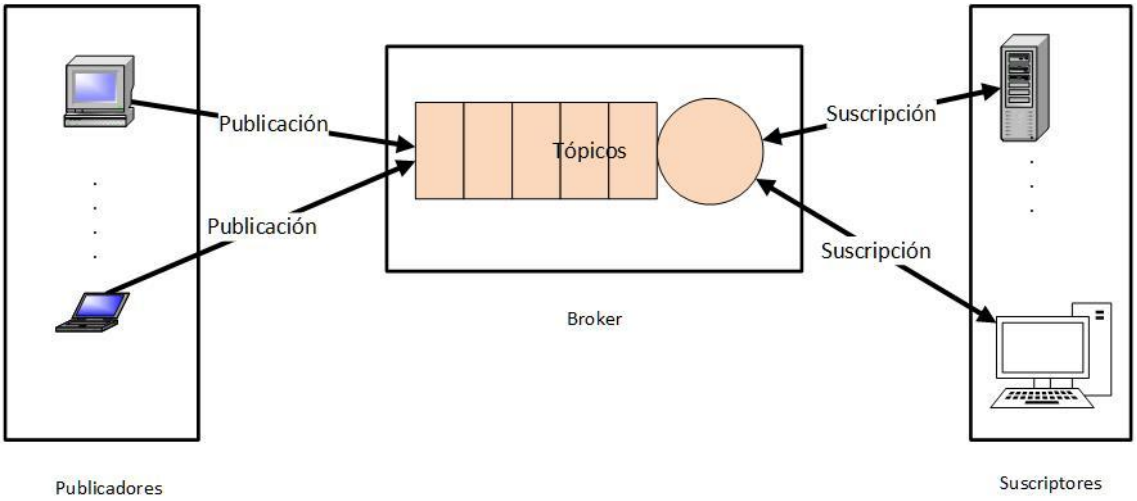


Ilustración 19: Arquitectura de MQTT

MQTT se compone de tres elementos: subscriber, publisher y broker. Un dispositivo se registra como subscriber en un tema en concreto para que sea informado por el bróker, cuando el Publisher publique temas de su interés. El Publisher transmite la información a las entidades interesadas (subscribers) a través del broquer. El bróker comprueba que ambos, subscribers y publishers, estén autorizados. Numerosas aplicaciones utilizan MQTT, salud, monitorización, medida de energía y notificaciones Facebook. El protocolo MQTT representa un protocolo de mensajes ideal para IoT y comunicaciones M2M y es capaz de proporcionar enrutamiento en dispositivos pequeños, de bajo consumo y memoria, en entornos hostiles y de baja tasa de trasmisión.

Los primeros dos bytes del mensaje son fijos, en este formato el valor del campo Message Type indica una variedad de mensajes que incluye. CONNECT(1), CONNACK(2), PUBLISH(3) y así sucesivamente. DUP indica que el mensaje está duplicado y que el receptor puede haberlo recibido antes. El campo QoS identifica los tres posibles niveles de QoS para la entrega de mensajes. El campo Retain instruye al servidor para que retenga el último mensaje recibido y que lo envíe a los nuevos subscribers como el primer mensaje.

0 1 2 3	4	5 6	7
Message Type	UDP	QoS Level	Retain
Remaining Length (1~4 bytes)			
Variable Length Header (Optional)			
Variable Length Message Payload (Optional)			

Ilustración 20: Mensaje MQTT.

4.2.4.4. Extensible Messaging and Presence Protocol (XMPP).

XMPP[12] es un estándar de la IETF de mensajería instantánea, utilizado para multichat, telepresencia y llamadas de voz y video. El Jabber open source community, lo desarrolló como un protocolo de mensajería abierto, seguro, libre de spam y descentralizado. Permite a los usuarios comunicarse entre sí, enviando mensajes instantáneos

sobre Internet, sin importar que sistema operativo se esté utilizando, además permite a las aplicaciones de mensajería instantánea control de acceso, autenticación, cifrado hop-by-hop y end-to-end, privacidad y compatibilidad con otros protocolos.

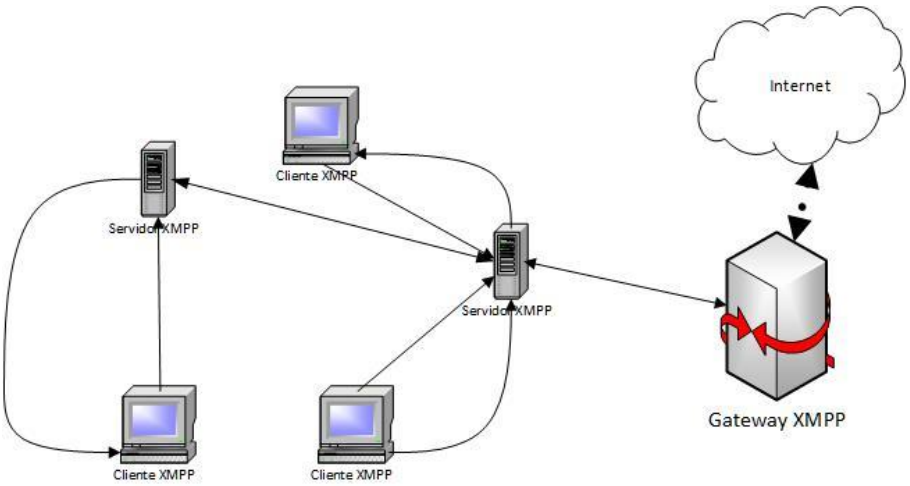


Ilustración 21: Comunicaciones en XMPP

Muchas de las características de XMPP lo hacen que sea un protocolo idóneo para aplicaciones de mensajería instantánea, y relevante dentro de IoT. Puede ejecutarse sobre una gran variedad de plataformas basadas en Internet, de forma descentralizada. Es seguro y permite la adición de nuevas aplicaciones encima del protocolo principal.

XMPP conecta al cliente a un servidor utilizando flujos de stanzas XML. Una stanza XML es una unidad semántica discreta de información estructurada que se envía de una entidad a otra a través de una secuencia XML. Representa un trozo de código que está dividida en tres componentes: menssage, presence e iq (info/query).

- Las stanzas message identifican la dirección de origen y destino, tipos e IDs de las entidades XMPP que utilizan un método push para recuperar datos. Una stanza message completa los campos asunto y cuerpo con el título del mensaje y su contenido.
- La stanza presence muestra y notifica a los clientes las actualizaciones de estado.
- La stanza iq empareja los remitentes y receptores de mensajes.

La comunicación está basada en texto mediante XML, lo que impone una sobrecarga de red bastante alta. Una solución a este problema es comprimir flujos XML utilizando EXI (Efficient XML Interchange). EXI logra de forma general, flexibilidad y rendimiento, unificando conceptos de la teoría del lenguaje formal y la teoría de la información en un solo algoritmo relativamente simple. El algoritmo utiliza una gramática para determinar lo que es probable que ocurra en cualquier punto determinado en un documento XML y codifica las alternativas más probables en menos bits. El algoritmo completamente generalizado funciona para cualquier lenguaje que pueda ser descrito por una gramática (por ejemplo, XML, Java, HTTP, etc.); Sin embargo, EXI está optimizado específicamente para los lenguajes XML.

```
<stream>
    <presence>
            <show>
    </presence>
<message to='x'>
            <body/>
    </message>
    <iq to='y'>
    <query/>

    </iq>
<stream>
```

Ilustración 22: Estructura de una stanza XMPP

4.2.4.5. Advanced Message Queuing Protocol (AMQP).

AMQP es un protocolo abierto, diseñado como un protocolo de aplicación estándar, disponible para el intercambio de mensajes entre distintas plataformas.

El objetivo de AMQP es asegurar que la información se transporta de forma segura y eficiente entre aplicaciones, entre organizaciones, a través de entornos distribuidos de computación en nube y dentro de infraestructuras móviles. AMQP evita las tecnologías propietarias, ofreciendo el potencial de reducir el costo de las integraciones de software middleware empresarial a través de la interoperabilidad abierta.

Las principales características de AMPQ, entre otras, son:

- Protocolo del nivel de aplicación del modelo OSI.
- Basado en el protocolo de transporte TCP de la pila TCP/IP.
- Orientado a mensajes.
- Enrutamiento punto a punto y publicación/suscripción.
- Comunicaciones seguras.

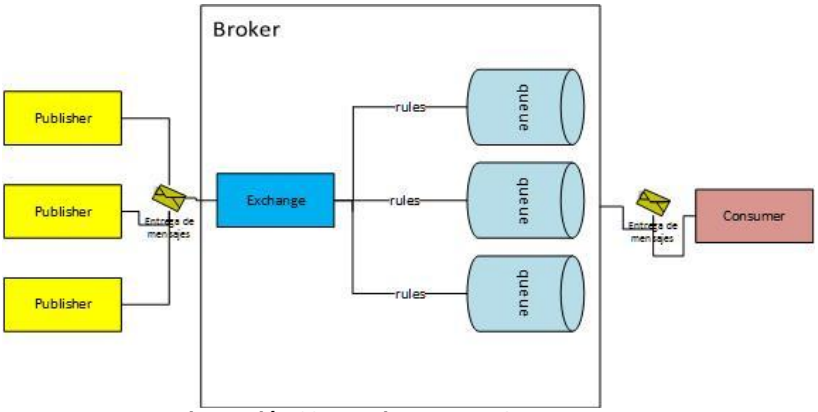


Ilustración 23: Arquitectura AMQP.

Define un protocolo de transporte (wire protocol) como una capa semántica de alto nivel de manera que distintas implementaciones de AMQP pueden ser capaces de operar unas con otras. La comunicación se realiza con dos componentes principales como se observa en su arquitectura: exchanges (intercambiadores) y queues (colas). Los

exchanges se utilizan para enrutar mensajes a las colas apropiadas mediante reglas y condiciones. Los mensajes pueden almacenarse en las colas de mensajes y enviarlos a los consumidores, además de este tipo de comunicación, AMQP permite el modelo publicación/suscripción.

AMQP, define un nivel de mensajería encima de su capa de transporte. Las diferentes posibilidades de mensajería son gestionadas dentro de este nivel, con dos tipos de mensajes: bare message, proporcionados por el emisor, y annotated messages que son vistos por el receptor.

El nivel de transporte proporciona los puntos de extensión necesarios para el nivel de mensajes, en este nivel, las comunicaciones son orientadas a paquetes. La estructura de un paquete es la siguiente: los primeros cuatro bytes muestran el tamaño, DOFF (data offset) da la posición del cuerpo dentro del paquete, el tipo field indica el formato y propósito del paquete, 0x00 se utiliza para mostrar que el paquete es AMQP, 0x01 representa una trama SASL

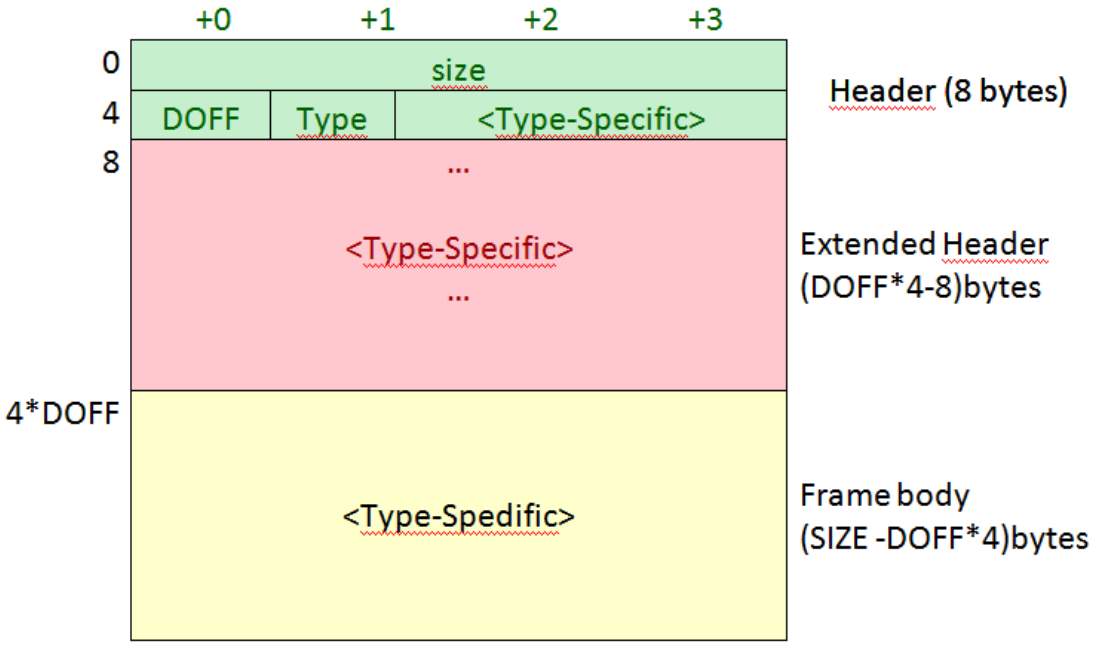


Ilustración 24: Formato de la trama AMQP

4.2.4.6. Data Distribution Service (DDS).

El Servicio de Distribución de Datos para Sistemas en Tiempo Real (DDS)[14] es un estándar de comunicación de datos del tipo publicación/suscripción del Object Management Group (OMG) para Internet de Cosas (IoT) e Industrial Internet of Things (IIoT).

DDS permite intercambio de datos escalable, en tiempo real seguro y de alto rendimiento, entre publicadores y suscriptores. Está diseñado para satisfacer las de necesidades de las aplicaciones IoT e IIoT (Industrial IoT), como control de tráfico aéreo, gestión de transportes, salud, energía y aplicaciones de big data.

Es a la vez un lenguaje y un sistema operativo. Las APIs (application programming interface) especificadas por el estandar se han desarrollado en diferentes lenguajes de programación: Ada, C, C++, C#, Java, JavaScript, CoffeScript, Scala, Lua y Ruby. Así, utilizando APIs estandarizadas se asegura que las aplicaciones DDS pueden portarse fácilmente.

A diferencia de otras tecnologías centradas en el mensaje (message-centric), DDS es una tecnología centrada en el dato (data-centric). Aunque ambas tecnologías data-centric y message-centric parecen lo mismo ya que proporcionan conectividad en sistemas distribuidos, la forma en que lo hacen es diferente. En un sistema centrado en el mensaje el interés está en la entrega del mensaje independientemente del contenido, mientras que en un sistema centrado en el dato el interés está en los datos del usuario.

La unidad de intercambio en este tipo de sistemas es el valor del dato, el sistema entiende el contexto del dato y se asegura que todos los suscriptores interesados tienen una visión correcta y consistente. En un concepto similar al de base de datos, que puede proporcionar una vista global de los datos y puede gestionar su acceso.

Una de las ventajas clave de las tecnologías centradas en el dato como DDS es que los datos compartidos permiten un nivel muy alto de abstracción para los usuarios.

A diferencia de otros protocolos como MQTT o AMQP, DDS no depende de un broker y se basa en la idea de “espacio global de datos” donde los productores escriben al espacio de datos y los consumidores leen del espacio de datos. Utiliza multicast, proporcionando una excelente QoS y alta confiabilidad a las aplicaciones. Su arquitectura responde bien a las restricciones de comunicación de IoT y M2M. Soporta 23 políticas de QoS mediante las cuales gran variedad e criterios de comunicación como seguridad, urgencia, prioridad, durabilidad, fiabilidad pueden ser seleccionadas por los desarrolladores.

La arquitectura DDS define dos niveles: Data-Centric Publish-Subcribe (DCPS) y Data-Local Reconstruction Layer (DLRL). DCPS es el encargado de la entrega de información a los subscribers, por otro lado DLRL, es opcional y es el interface para las funcionalidades DCPS. Facilita el intercambio de datos distribuidos entre objetos.

Existen cinco entidades involucrada con el flujo de datos dentro del nivel DCPS:

- Publisher que disemina los datos.
- DataWriter, la aplicación lo usa para interactuar con el Publisher sobre los valores y cambios de datos específicos a un tipo determinado.
- Subscriber que recibe datos publicados y los entrega a la aplicación
- DataReader, el Subscriber lo emplea para acceder a los datos recibidos.
- Un Tópico que es identificado por un tipo de datos y un nombre.

La transmisión de datos se permite dentro de un dominio DDS que es un entorno virtual para aplicaciones de publicación suscripción conectadas.

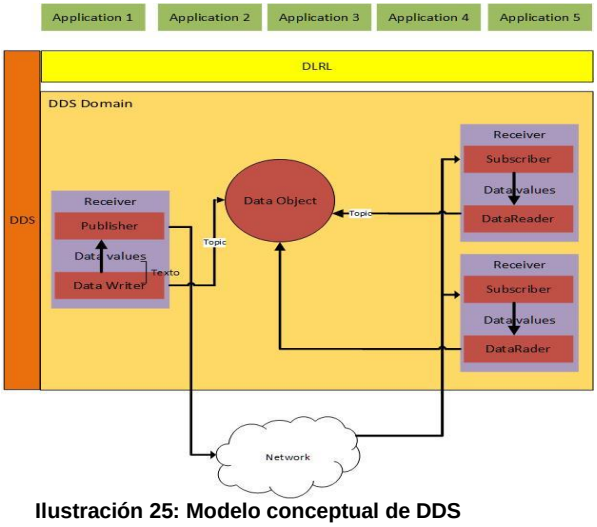


Ilustración 25: Modelo conceptual de DDS

A continuación mostramos una comparativa de los protocolos citados:

Protocolos de aplicación	RESTFul	Transporte	Publicación/ suscripción	Petición/respuesta	QoS	Tamaño cabecera
HTTP	Si	TCP	No	Si	No	
CoAP	Si	UDP	Si	Si	Si	4 bytes
MQTT	No	TCP	Si	No	Si	2 bytes
XMPP	No	TCP	Si	Si	No	
AMQP	No	TCP	Si	No	Si	8 bytes
DDS	No	TCP/UDP	Si	No	Si	

Ilustración 26: Comparación protocolos nivel aplicación

4.3. LPWA networks.

LPWA es el acrónimo de Low Power Wide Area, que designa una tecnología de red caracterizada por:

- Conectar dispositivos de bajo consumo, equipados con baterías con duración de varios años.
- Conectar dispositivos con bajos requerimientos de ancho de banda.
- Operar a grandes distancias.

Diseñadas para entornos M2M, las LPWA permiten una gama más amplia de aplicaciones M2M y de IoT que las redes celulares. Las tasas de transferencia son muy bajas, por lo que el consumo de energía de los dispositivos conectados es también muy bajo. Permite la conexión de dispositivos que necesitan menor ancho de banda del que requieren dispositivos utilizados normalmente en el hogar, además estas redes

pueden operar a menor coste, con mayor eficiencia energética y admitir un mayor número de dispositivos, de los que lo hacen las tecnologías móviles.

Los dispositivos capaces de conectarse a estas redes son de bajo coste y de muy bajo consumo, dejando la complejidad de las comunicaciones en las estaciones base, ya que actualmente estas no tienen limitación de consumo energético.

Las tecnologías LPWA representan la respuesta de la industria a la creciente necesidad del mercado de una conectividad barata y de bajo ancho de banda para aplicaciones IoT que no son adecuadas para opciones inalámbricas de corto alcance como Bluetooth o ZigBee. Más allá de la cobertura, las aplicaciones de IoT también requieren un mecanismo de despliegue más simple que el de las tradicionales tecnologías de corto alcance, ya que dependen de redes locales más complejas, lo que implica la gestión de credenciales de seguridad, las conexiones entre varios fabricantes y la calidad de la conexión.

Las tecnologías LPWA poseen el potencial para simplificar el despliegue de dispositivos de bajo consumo, ideales para muchas aplicaciones Smart City y aplicaciones IoT de nueva generación, con lo que la conectividad de dispositivos electrónicos que se incorporan en alguna parte de nuestro cuerpo, interactuando de forma continua con nosotros y con otros dispositivos, con la finalidad de realizar alguna función concreta, como pueden ser los relojes inteligentes o smartwatchs, las zapatillas de deportes con GPS incorporado y pulseras que controlan nuestro estado de salud, son ejemplos, entre otros muchos, de este género tecnológico que se halla poco a poco más presente en nuestras vidas.

Características de las redes LPWA		
Característica	Orden de magnitud	Valor
Espectro	No licenciado	<1GHz/2,4GHz
Rango	Largo	10-50+km(rural)/0-5km(urbano)
Objetos	Muchos	Muchos miles
Volumen de datos	Pequeño	Mas de 10kb por día
Ratio de datos	Bajo	De 100 a 100 kb/s
Latencia	De abajo a arriba	Más que minutos
Vida de la batería	Larga	Más de 20 años
Coste del módulo	Bajo	<5 €
Coste del servicio	Bajo	<10€ por año

Ilustración 27: Características de las redes LPWA

El despliegue masivo de dispositivos de bajo consumo supone una serie de desafíos y retos que incluyen:

- Duración de la batería: la mayoría de los dispositivos IoT están alimentados por baterías y el coste de sustituir las baterías en

numerosos dispositivos situados en lugares de difícil acceso puede no ser viable.

- Coste del dispositivo: los dispositivos deben de ser de un coste razonable que permita el despliegue de forma masiva.
- Cobertura: la cobertura es un requisito para la mayor parte de las aplicaciones, en áreas abiertas y en entornos cerrados.
- Diversidad: la conexión debe de ser capaz de permitir diferentes requerimientos, conexiones a dispositivos estáticos, móviles, con gran ancho de banda y baja latencia…
- Escalabilidad: el despliegue masivo de dispositivos necesita de redes que permitan soportar el aumento de los mismos de manera eficiente y sin pérdida de funcionalidad.

Internet de las cosas (IoT) ha cambiado fundamentalmente la naturaleza de los dispositivos conectados, creando tecnologías de red de área amplia de baja potencia (LPWAN). Las soluciones LPWAN son ideales para dispositivos que necesitan enviar cantidades de datos sobre grandes distancias, con restricciones en el consumo de energía y capacidad de proceso.

Dada la necesidad inmediata de LPWAN en los despliegues de IoT, han surgido múltiples soluciones que ofrecen el equilibrio adecuado entre ancho de banda, consumo de energía y cobertura a un costo razonable. Algunas de estas iniciativas son coordinadas por alianzas de estándares, mientras que otras lo son por compañías privadas con soluciones patentadas. Aunque existen tecnologías como Bluetooth y ZigBee, ya comentadas, solucionan a menudo problemas similares, no son tecnologías LPWAN.

Existen gran cantidad de protocolos LPWAN, a continuación mostramos algunos y una breve descripción:

LoRaWAN™

Estándar abierto de LoRa Alliance, aunque no totalmente. Es la especificación de una red de área extensa de baja potencia para dispositivos inalámbricos equipados con baterías dentro de una red regional, nacional o global.

SigFox.

Con una gran implantación en Europa, utiliza modulaciones lentas para conseguir grandes distancias. No es un protocolo abierto.

NWave.

Similar a SigFox en términos de funcionalidad, pero con una implementación mejor del nivel MAC (según NWave). Utiliza técnicas avanzadas de modulación para poder coexistir con otras tecnologías de radio.

Weightless

Es el único estándar totalmente abierto que opera en la banda no licenciada por debajo de 1 GHz. Existen tres versiones para diferentes propósitos:

- Weightless-W: aprovecha los espacios en blanco del espectro de la banda licenciada utilizada por la televisión.

- Weightless-N: protocolo de espectro no licenciado de banda estrecha, nacido de la tecnología Nwave.
- Weightless-P: Protoloco bidireccional nacido de la tecnología Platanus M2COMM

OnRamp.

RPMA (random phase multiple Access) es una combinación de tecnologías diseñadas específica y exclusivamente para comunicaciones M2M. Es una solución propietaria que permite mayores tasas de rendimiento que LoRa o SigGox.

4.3.1. Técnicas de diseño.

Podemos observar que existen multitud de tecnologías LPWAN que emplean diferentes técnicas para conseguir sus objetivos:

El éxito de las tecnologías LPWA radica en proporcionar conectividad a un gran número de dispositivos distribuidos sobre grandes áreas geográficas, a veces de difícil acceso, en entornos hostiles de propagación, a bajo costo y con consumo de energía limitado.

Cobertura.
Las tecnologías LPWA están diseñadas para tener un gran área de cobertura y una excelente propagación de la señal, difícil de conseguir en entonos de interior. Para permitir a los dispositivos conectarse a las estaciones base a distancias comprendidas entre unos pocos metros y decenas de km, es necesaria una ganancia de unos 20dB por encima de los sistemas de telefonía móvil.

Para conseguir este objetivo se ponen en juego el uso del espectro por debajo de la banda de 1 GHz y modulaciones especiales.

La mayoría de las tecnologías LPWA (a excepción de algunas) utilizan la banda por debajo de 1GHz (sub-1GHz), ya que permite mejor comunicación y más segura, con bajos consumos de energía. Comparado con la banda de 2,4 GHz, las señales de baja frecuencia sufren menor atenuación y efectos de multipath, además de estar menos congestionadas.

Las tecnologías LPWA se diseñan para conseguir enlaces de 150±10dB que permite distancias que van desde unos pocos km a decenas de km en entornos urbanos y aéreas rurales, respectivamente. En el nivel físico se compromete la velocidad de los datos disminuyendo la velocidad de modulación, para poner más energía en cada bit transmitido (o símbolo). De esta forma los receptores pueden decodificar señales correctamente, aunque estén muy atenuadas.

Dos son las técnicas de modulación adoptadas:

Modulación de banda estrecha (Narrowband).
Codifica la señal, generalmente con menos de 25KHz, de manera que se comparte el espectro de forma eficiente entre múltiples enlaces, además el nivel de ruido que se produce dentro de una banda estrecha es mínimo. Tampoco se necesita más capacidad de proceso a través del

desensanchado de la frecuencia para decodificar la señal en el receptor, abaratando los costes del mismo.

Algunas tecnologías LPWA introducen la portadora en bandas ultraestrechas (Ultra Narrow Band, UNB), de unos 100Hz de ancho, permitiendo reducir aún más el ruido y aumentando el número de dispositivos finales soportados por unidad de ancho de banda. No obstante, la tasa efectiva de datos de los dispositivos finales se reduce, aumentando el tiempo que la radio del propio dispositivo permanece encendida. La naturaleza de UNB aprovecha que la densidad de energía del ruido tienda a esparcirse (spread) a través del espectro, por lo tanto la señal UNB estará por encima del ruido. UNB utiliza canales RF permitiendo una alta sensibilidad del receptor y así extender el alcance a costa de una baja tasa de bits. Para cada transmisión (subida/bajada) utiliza canales distintos de banda estrecha, además el espectro que se utiliza se canaliza para que se produzcan varia subidas y bajadas de forma simultáneamente.

Técnicas de espectro ensanchado (spread spectrum).
Estas técnicas ensanchan una señal de banda estrecha, sobre una banda de frecuencias mayor manteniendo la misma densidad de potencia. La transmisión real es una señal similar al ruido, esta es más difícil de detectar, más resistente a las interferencias y más robusta a ataques de denegación de servicio contra el medio inalámbrico (jamming attacks). Sin embargo necesitan mayor capacidad de proceso en el receptor para decodificar una señal que se recibe por debajo del nivel de ruido. Se utilizan diferentes técnicas de espectro ensanchado como: Chirp Spread Spectrum (CSS)[20] y Direct Secuence Spread Spectrum (DSSS)[21].

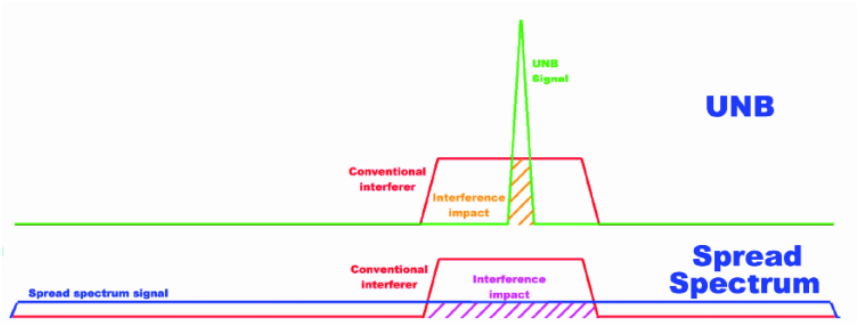


Ilustración 28: Comparación entre UNB y Spread Spectrum.

Funcionamiento de muy bajo consumo.

El consumo de energía es un factor clave para el despliegue y operación de dispositivos dentro de una red LPWAN. Topología, ciclo de trabajo, control de acceso al medio y descarga de la complejidad de los dispositivos finales, son aspectos de diseño que deben de tenerse en cuenta.

Topología.
Las topologías malladas presentan el problema que el tráfico se envía sobre múltiples dispositivos (hops) hacia una pasarela (Gateway), de manera que algunos nodos están más congestionados que otros dependiendo de su ubicación dentro de la red o las pautas de tráfico que

se produzcan. De manera que agotarán sus baterías rápidamente, limitando así el tiempo de vida de la red. Las tecnologías LPWA solucionan estas limitaciones conectando los dispositivos finales directamente a estaciones base, eliminando la necesidad de despliegue de repetidores y gateways. La topología es una estrella, donde los dispositivos no utilizan sus baterías para escuchar y transmitir el tráfico de otros dispositivos. Otras topologías utilizadas por LPWA son en árbol y malladas pero con una complejidad adicional en el diseño del protocolo.

Ciclo de trabajo.
Un duty cycle (ciclo de trabajo) es la fracción de tiempo de un periodo en el que una señal o sistema está activo (wikipedia). Los mecanismos de ciclo de trabajo de LPWA, se adaptan dependiendo de la aplicación, tipo de fuente de energía y pautas de tráfico, entre otros factores. Los dispositivos solo escuchan cuando la estación base transmite, o solo transmiten cuando los datos están listos para enviarse. Debido a las regulaciones del ciclo de trabajo en las bandas ISM, suponen un factor clave en la capacidad y el tamaño de la red como se expone en [22]

Control de acceso al medio.
Los protocolos estándar utilizados para el control de acceso al medio (Medium Access Control) en redes de telefonía móvil o redes wireless de corto alcance son demasiado complejos para LPWA, donde los esquemas simples de acceso aleatorio son más populares.

Diferentes tecnologías LPWA utilizan ALOHA, un protocolo de acceso al medio donde los dispositivos transmiten sin detección de portadora (carrier sensing). La simplicidad de ALOHA permite un diseño simple y bajo costo del transceiver. Otras tecnologías LPWA utilizan protocolos MAC basados en acceso múltiple por división en el tiempo (Time división multiple access, TDMA) para utilizar los recursos radio de forma más eficiente a costa de mayor complejidad y coste de los dispositivos.

Descarga de la complejidad de los dispositivos finales.
Descargar la complejidad de los dispositivos sobre las estaciones base, permite simplificar el diseño de los dispositivos finales ya que determinadas tareas son realizadas por las estaciones base, a costa de aumentar la complejidad de las mismas. Generalmente las estaciones base disponen de hardware diverso y son capaces de transmitir y recibir de múltiples dispositivos utilizando varios canales o señales ortogonales de forma simultánea.

El proceso de datos también puede eliminarse de los dispositivos, no obstante dependiendo de los requerimientos de la aplicación, se necesitará o no capacidad de proceso, lo que determinará la naturaleza de los datos transportados y de la complejidad del dispositivo.

Bajo coste.
Además de las técnicas mencionadas anteriormente: topología, uso de protocolos MAC y descarga de la complejidad de los dispositivos finales. Se utilizan otras estrategias para mantener un coste bajo:

- Reducción de la complejidad del software.

LPWA, a diferencia de otras tecnologías de corto alcance, utiliza transceivers que no necesitan procesar señales complejas, lo que se traduce en una menor complejidad y por ende el coste.

- Infraestructura mínima.

Las estaciones base LPWA pueden servir a cientos de dispositivos, distribuidos en un área más amplia que las utilizadas en tecnologías tradicionales, reduciendo así el coste de la infraestructura desplegada.

- Uso de bandas no licenciadas o licenciadas.

Muchas de las tecnologías LPWA utilizan frecuencias no licenciadas evitando el coste que representan las tasas correspondientes. Por otro lado existe una tendencia, en determinadas tecnologías LPWA, a utilizar bandas licenciadas para evitar la degradación producida debido el incremento de dispositivos compartiendo el espectro.

Técnicas de diversidad.

Las tecnologías LPWA utilizan comunicaciones multicanal y multiantena para paralelizar las transmisiones con los dispositivos, para hacer las comunicaciones resistentes a las interferencias, se utilizan varios canales y transmisiones redundantes.

Selección de canal y tasa de datos variable.

Se necesita monitorizar eficientemente la calidad de los enlaces y coordinación entre los dispositivos y la red, de manera que puedan utilizarse diferentes esquemas de modulación, seleccionar los mejores canales o realizar transmisiones que se adapten al consumo de energía.

Calidad de servicio.

Las aplicaciones que hacen uso de las tecnologías LPWA poseen diferentes necesidades. Unas necesitan un mínimo de latencia en la entrega de datos, mientras que otras pueden tolerar cierta latencia. Es necesario pues que establezcan los mecanismos de calidad de servicio.

4.3.2. Tecnologías LPWA a estudio: SigFox y LoRa

Una vez vistas las principales características de las tecnologías LPWA, sus condicionantes de diseño y algunas de las soluciones posibles, vamos a mostrar las características particulares de SigFox y LoRa.

4.3.2.1. SigFox

Es una variación del sistema celular que permite a dispositivos conectarse a un punto de acceso con UNB. Es una tecnología propietaria, desarrollada por la compañía Francesa Sigfox, que no publica las especificaciones. Utiliza 200 KHz de bandas no licenciadas (ISN) para intercambiar mensajes de radio. Las frecuencias, dependiendo de las regiones, son 868 a 870 MHz y 902 a 928 MHZ. Combina UNB con modulaciones DBPSK y GFSK [17], con un ancho de 100 MHz por mensaje, transmitidos a 100 o 600 bps dependiendo de la zona.

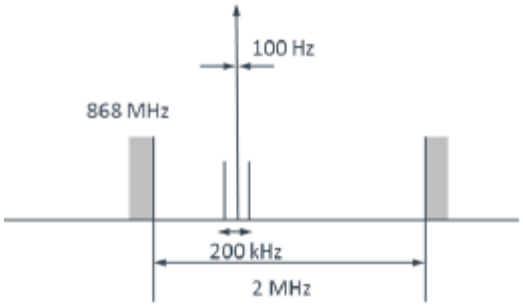


Ilustración 29: Uso de ancho de banda

Los mensajes que se transmiten por SigFox, son pequeños, con 12 bytes en el enlace de subida y 8 bytes en el de bajada. El protocolo transmite el ID del dispositivo, de manera que los 12 y 8 bytes representan la carga útil (payload). Para una carga útil de 12 bytes, una trama SigFox utiliza 26 bytes en total.

Con 12 bytes se cubren las necesidades de transmisión de los dispositivos (localización, consumo, alarma o cualquier tipo de información básica que proporcione un sensor). Con 8 bytes para la recepción se puede enviar al dispositivo datos de configuración. La red ofrece diferentes modalidades de transmisión basándose en el número de dispositivos y el número de mensajes transmitidos al día.
Un dispositivo puede transmitir a cualquier lugar dentro de la banda de operación, la transmisión no está sincronizada entre el dispositivo y la red. El dispositivo emite cada mensaje 3 veces en 3 frecuencias diferentes (salto de frecuencia). Las estaciones base monitorizan el espectro buscando señales UNB para demodular.

Tras la transmisión del mensaje en la primera frecuencia, el dispositivo cambia al modo de recepción para intentar recibir un mensaje desde la estación base. El tiempo máximo de espera, para la recepción, es de 25 segundos. No puede enviase un nuevo mensaje, desde el dispositivo dentro de los seis segundos posteriores a la recepción de un mensaje.
Los dispositivos puede enviar entre 0 y 140 mensajes al día, esto supone que solo se puede enviar un mensaje cada 11 minutos en 24 horas.

La red permite diferentes modalidades, basándose en el número de dispositivos y el volumen de mensajes por día [15]:

- Platinum: de 101 a 140 mensajes + 4 enlaces de descarga.
- Gold: de 51 a 100 mensajes + 2 enlaces de descarga.
- Silver: de 3 a 50 mensajes + 1 enlace de descarga.
- One: de 1 a 2 mensajes sin descarga.

En la región 1 de la ITU, la banda 868 está sujeta a limitaciones en el ciclo de trabajo, en este caso, el ciclo de trabajo máximo es del 10%, que representa el máximo de 140 mensajes/día para la modalidad platinum

La pila de protocolos Sigfox es el software utilizado por los dispositivos conectados para generar tramas de radio y así transmitir mensajes a través de la red global de Sigfox. Se proporciona de forma gratuita a los fabricantes. Está incrustado en millones de chipsets, sistemas en chips o módulos. Cabe destacar el uso de R-FDMA, como esquema de acceso al medio [16]

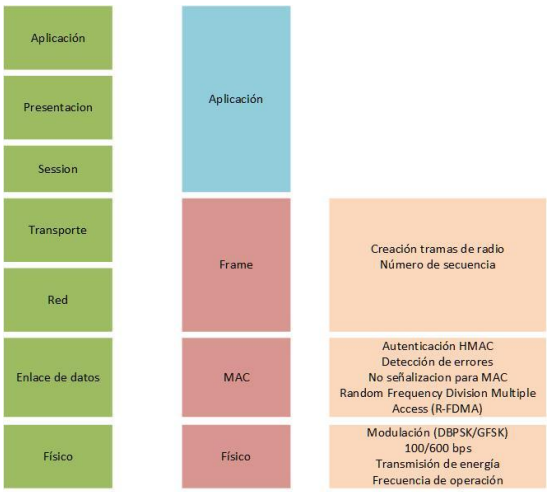


Ilustración 30: Pila de piocolos Sigfox comparada con el modelo OSI

La arquitectura de red se basa en la topología en estrella, donde un dispositivo no está conectado a una estación base especifica, a diferencia de los protocolos de dispositivos celulares. Los mensajes se reciben en cualquier estación base, dentro del rango de alcance, que es de tres estaciones de media.

Los componentes de la red de Sigfox son:

- Objetos, transmiten mensajes a la red SigFox.
- Estaciones Sigfox, están conectadas directamente al Cloud de Sifox, mediante enlaces punto a punto, y reciben los mensajes de los objetos. Detectan y demodulan los mensajes, para posteriormente enviarlos al Cloud.
- Cloud de Sigfox, envía los mensajes a la plataforma del cliente.
- Plataforma del cliente, recibe los mensajes de los objetos a través de la red se SigFox.

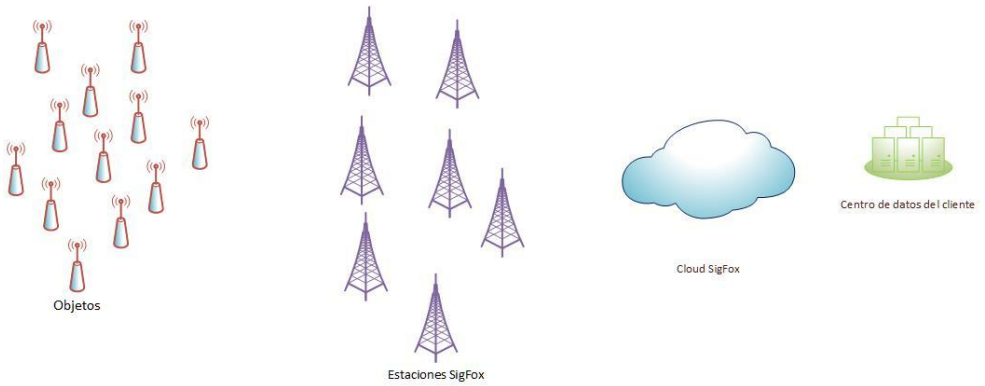


Ilustración 31: Arquitectura Sigfox

4.3.2.2. LoRa.

Se trata de una especificación LPWAN para dispositivos IoT, con un alcance regional, nacional o global. Puede operar en 433, 868 o 915 MHz dependiendo de la zona de operación. En Europa emplea GFSK o un esquema de modulación propietario de LoRa, que utiliza una versión de CSS con un ancho de canal de 125 KHz. La carga útil puede ser de 2 hasta 255 bytes.

La topología de la red es una estrella jerárquica, donde se envían mensajes a un servidor central utilizando gateways. La tasa de transmisión puede ir de 300 bps hasta 50 Kbps empleando agregación de canales.

Generalmente LoRa hace referencia a dos niveles [19]:

- Un nivel físico que utiliza CSS como técnica de modulación.
- Un nivel de acceso al medio (LoRaWAN).

Ilustración 32: LoRa y LoRaWAN dentro del modelo OSI

El nivel físico, desarrollado por Semtech, permite largo alcance, bajo consumo de energía y baja tasa de datos, en el rango de frecuencias y con las características de los mensajes ya comentadas.

LoRa (Long Range) es una técnica de modulación basada en técnicas de espectro ensanchado y una variación de CSS con corrección de errores FEC (forward error correction). Utiliza todo el ancho de banda del canal para enviar la señal, haciéndola resistente al ruido y al desplazamiento de frecuencia producido por el uso de cristales de bajo coste. LoRa puede demodular señales 19,5dB por debajo del suelo de ruido, mientras que normalmente los sistemas FSK (frequency shift keying) necesitan una señal de entre 8 y 10 dB por encima del suelo de ruido para poder demodular la señal correctamente.

LoRaWAN, proporciona un mecanismo MAC, para permitir a los dispositivos comunicarse con un gateway utilizando la modulación que proporciona LoRa.

Mientras que la modulación es propietaria, LoRaWAN es un estándar abierto desarrollado por la LoRa Alliance.

La arquitectura básica de una red LoRaWAN es la siguiente:

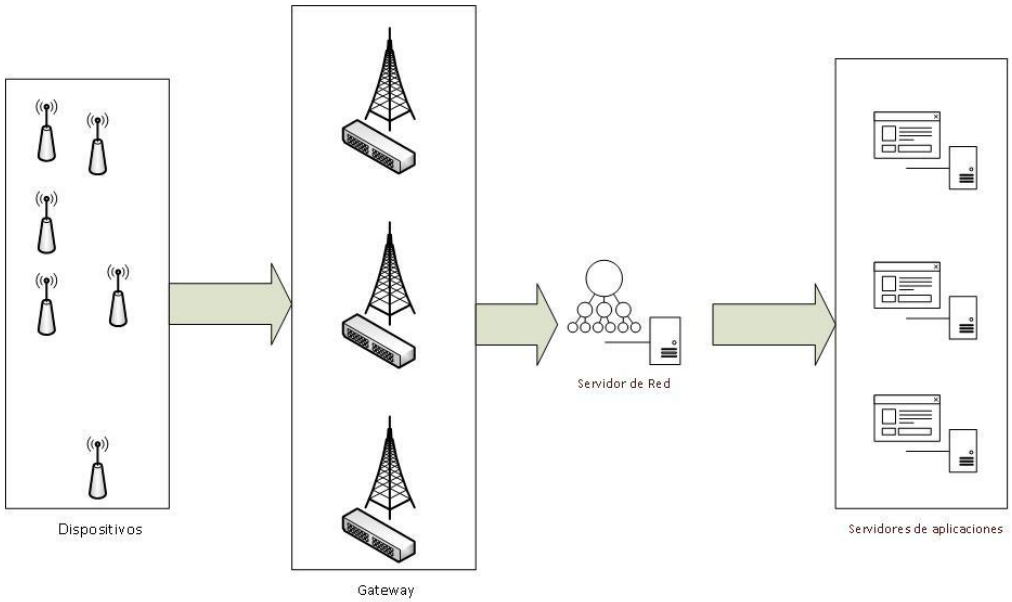


Ilustración 33: Arquitectura LoRA

Los dispositivos se comunican con gateways utilizando LoRa con LoRaWAN. Los gateways transmiten los datos en crudo (raw data) de los dispositivos hasta un servidor sobre una interfaz de backhaul, que suele ser Ethernet o 3G. Como puede observarse los gateways son sólo relés bidireccionales o convertidores de protocolo, siendo los responsables de descodificar los paquetes enviados por los dispositivos y generar los paquetes que deberían ser devueltos a los dispositivos.

Existes tres clases de dispositivos finales que solo se diferencian en la forma en la que se programa el enlace descendente.

- Clase A (enlaces bidireccionales): cada transmisión del dispositivo hacia el gateway va seguida por dos ventanas de recepción de

corta duración. Los dispositivos de clase A utilizan la más baja energía y son útiles para aplicaciones donde la comunicación hacia el dispositivo no es crítica.

- Clase B (comunicaciones bidireccionales con periodos de recepción planificados): además de las dos ventanas de recepción los dispositivos de clase B planifican conexiones de sincronización para que el servidor sepa que dispositivo está escuchando.
- Clase C (comunicaciones bidireccionales con ventanas de recepción máximas): los dispositivos de clase C, disponen de ventanas de recepción que solo se cierran cuando el dispositivo transmite. Utiliza gran cantidad de energía y proceso por lo que no es apto para aplicaciones de bajo consumo.

	LoRa	Sigfox
Banda de operación	SUB-GHZ ISM:EU (433MHz-868MHz), US (915MHz), Asia(430MHz)	SUB-GHZ ISM:EU (868MHz), US(902MHz)
Tasa de datos	0.3-37.5 kbps (LORa), 50 kbps (FSK)	100 bps(EA), 600 bps(ED)
Alcance	5 km(URBANO), 15 km (RURAL)	10 km (URBANO), 50 km (RURAL)
Enlace simétrico	Si	No
MAC	ALOHA	ALOHA
Topología	Estrella de estrellas	Estrella
Enlace Ascendente	Datos	Datos
Enlace Descendente	Datos + ACK	ACK
Carga útil	19-250 bytes	12 bytes
Carga de protocolo	12 bytes	26 bytes
Potencia de TX	13dBm	14dBm
Consumo en TX	28mA	10mA
Consumo en RX	10,5mA	10mA
Modulación	CSS/FSK/OOK/GMSK	GFSK/BPSK
Sensibilidad (dBM)	-137	-129

Ilustración 34: Características LoRa, SigFox

4.3.3. Despliegue de redes LPWA en España.

En España, la tecnología Sigfox ha tomado la delantera claramente en el despliegue de redes LPWA, al disponer ya de una red operativa que cubre toda la geografía española, pudiendo así los usuarios comprar dispositivos certificados Sigfox para usarlos.

Este despliegue lo ha llevado a cabo Cellnex Telecom(antigua Abertis) [23]. Cellnex Telecom es un operador independiente líder de emplazamientos de telecomunicaciones inalámbricos de Europa, con una cartera única de torres de telecomunicaciones y radiodifusión, que le ha permitido realizar el despliegue de una red LPWA, por todo el país,

utilizando SigFox. Cellnex también desarrolla soluciones en la campo de smart city y está firmemente comprometida con el desarrollo de su red a través de la adquisición de torres de telefonía móvil. Existen más de 1.400 estaciones base que proporcionan una cobertura que es significativamente mayor que en otros países que han desplegado este tipo de redes. Esta red ha permitido el desarrollo de nuevos productos como las alarmas de hogar de nueva generación "VeriSure" desarrolladas por Securitas Direct. En la actualidad, hay más de 500.000 objetos conectados.

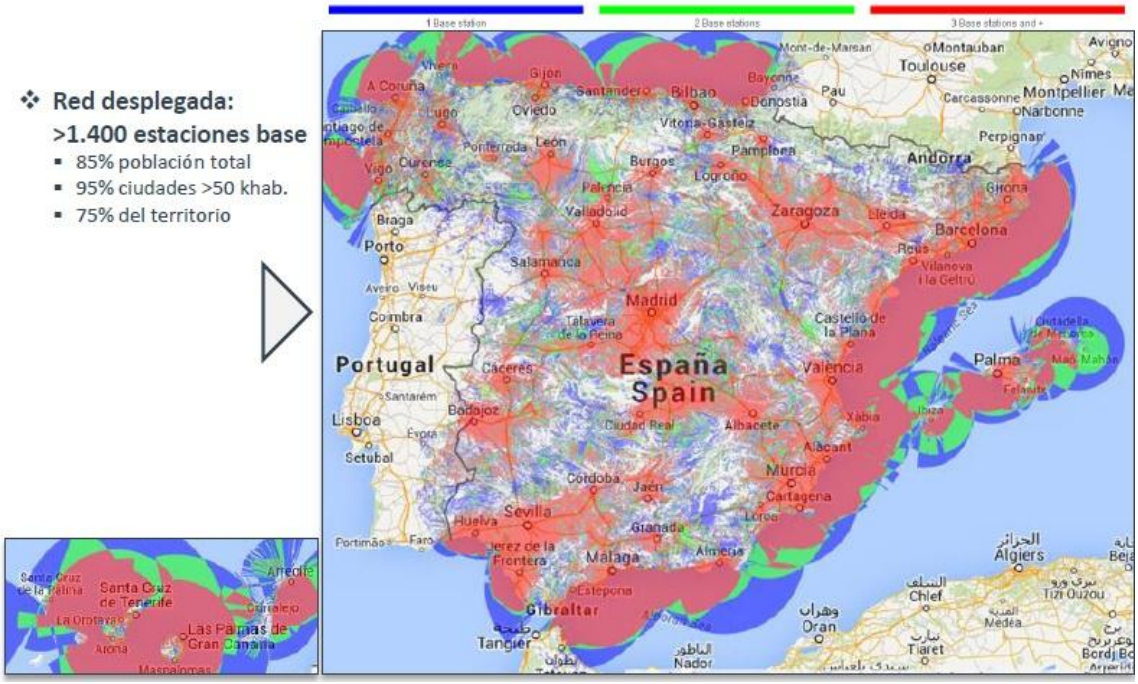


Ilustración 35: Despliegue de la red de Cellnex-Telecom

Existen otras iniciativas de operadores de telefonía móvil, como la de Vodafone [24] que anuncia el lanzamiento de la primera NB-IoT (Banda Estrecha de internet da las Cosas) del país, disponible en seis grandes ciudades.

4.4. Sistemas M2M celulares.

Ante el auge de IoT, los operadores de redes móviles están tomando una posición de liderazgo en el impulso del IoT, proporcionando conectividad a una amplia gama de dispositivos inteligentes y soluciones conectadas para casas, hospitales, fábricas, coches y otros medios de transporte. Las ventajas económicas y sociales de estas soluciones conectadas han dado lugar a una rápida expansión del IoT, hasta el punto en el que los requisitos de espectro del ecosistema superan la capacidad. Conforme los gobiernos están asignando más licencias de espectro para favorecer el crecimiento del IoT, el rol de los operadores se vuelve incluso más importante a la hora de dar forma al Internet de las cosas. Las operadoras de telefonía móvil ofrecen plataformas integrales de IoT seguras que permiten a los clientes escalar y gestionar

sus necesidades de negocio. También cuentan con una cobertura de red global inigualable, así como con un soporte técnico y empresarial para reaccionar a las necesidades cambiantes de los clientes.

La GSMA (organización de operadores móviles y compañías relacionadas, dedicada al apoyo de la normalización, la implementación y promoción del sistema de telefonía móvil GSM) anunció en agosto de 2015 que la industria móvil había acordado la "Iniciativa IoT móvil" creada para acelerar la disponibilidad comercial de soluciones LPWA en el espectro autorizado.

Las especificaciones iniciales de las soluciones LPWA se han incluido en la versión 13 de 3GPP (3rd Generation Partnership Project)[28], definiendo una nueva categoría de UE (user terminal) con un conjunto de recomendaciones estándar para dispositivos de bajo coste, baja complejidad y ancho de banda reducido, para comunicaciones MTC (Machine-Type Communicactions), que permita de alguna manera la idoneidad de LTE (long term evolution) en el creciente mercado de IoT .

4.4.1 Tecnología 3GPP.

La tecnología LTE Cat-M1 [25] es una de las dos respuestas que 3GPP tiene para IoT. LTE-M es la abreviatura de LTE Cat-M1 o Long Term Evolution (4G), categoría M1. Esta tecnología se desarrolla para permitir que dispositivos de Internet de cosas puedan conectarse directamente a una red 4G.

Las especificaciones de LTE CAT-M1 (3GPP release 13) son, entre otras:

- Batería de 5WH de 10 años de vida.
- Coste del dispositivo comparable a dispositivos IoT basados en GPRS.
- Cobertura extendida, > 156 dB MCL (minimum coupling loss)
- Tasa de datos variable para mejorar la cobertura

En la actualidad LTE-M es una tecnología que está empezando a desplegarse, en Estados Unidos, Verizon ha realizado un gran esfuerzo para lanza la red LTE-M1 [26].

La otra respuesta del 3GPP es NB-IoT, que usa un esquema de acceso más simple que el anterior, SC-FDMA (Single Carrier Frequency Division Multiple Access), para reducir el coste y la complejidad. NB-IoT, se ha desarrollado para reutilizar el diseño de LTE [27] y para permitir una integración fácil y compartir los recursos radio con las redes GSM y LTE existentes, que no operará en LTE. Se está diseñando, de manera que exista de una de las siguientes maneras:

- De forma independiente.
- En la banda de 200 KHz, previamente utilizada por GSM.
- En estaciones base LTE, que asignan un bloque de recursos a las operaciones NB-IoT o en sus bandas de protección.

En la siguiente tabla se resumen las diferentes tecnologías descritas y su correspondencia con el modelo OSI

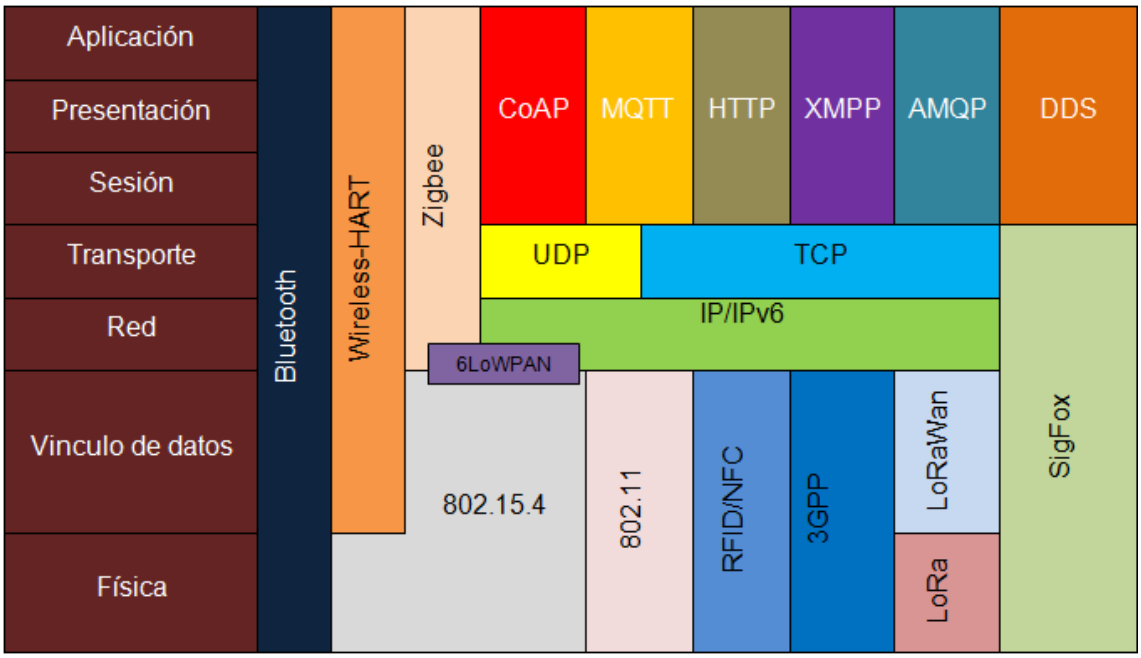


Ilustración 36: Tecnologías expuestas en la pila ISO

4.5 Opinión sobre las tecnologías expuestas.

Con la aparición de IoT, han surgido una serie de tecnologías, algunas nuevas, otras evolucionadas de otras que ya existían, que ofrecen varias opciones de conectividad, plataformas y tecnologías para los desarrolladores. Aunque algunos componentes pueden utilizarse en diferentes escenarios, cada aplicación tiene requisitos y restricciones específicos que deben tenerse en cuenta. Dados los extremos potenciales, en estas situaciones, el fracaso puede resultar en una inversión significativa para reparar o reemplazar el sistema e incluso poner vidas humanas en riesgo. La clave es entender completamente las metas y los requisitos de cada sistema para que pueda poner en foco todas las diversas opciones y seleccionar la tecnología correcta para cada circunstancia única.

Por ejemplo, aunque a priori, utilizar UDP como transporte puede que se ajuste a las necesidades de bajo consumo y baja tasa de datos, puede no ajustarse a las necesidades de nuestro sistema, en el caso de requerir cierta fiabilidad. Utilizar un bróker puede parecer, un elemento prescindible, pero si nuestro sistema tiene decenas de miles de dispositivos, puede ser complicado enviar un mensaje de reinicio a todos ellos de forma simultánea.

Utilizar tecnologías abiertas, permite diseñar sistemas independientes cuyo desarrollo no pertenece a ninguna empresa, con tecnologías basadas en estándares regulados por un comité compuesto por numerosos miembros y entidades. Generalmente son más baratas que las propietarias y permiten un alto nivel de control del sistema a los desarrolladores.

Por otro lado las tecnologías propietarias ofrecen un nivel de seguridad que no ofrecen las abiertas, al ser precisamente propietarias y su tecnología no depender de estándares.

4.5.1. Factores a tener en cuenta en la evaluación de tecnologías en el diseño de sistemas IoT.

- Crecimiento. Evaluar los costos de la compra inicial y de la ampliación, una de las preocupaciones para la elección de la tecnología debería ser no sólo en la compra inicial, sino también en los costos de la incorporación de nuevos elementos.
- Avances tecnológicos. Un sistema con tecnologías que no evolucionan se vuelve obsoleto en poco tiempo, disminuyendo la duración de la inversión y generando costos operativos adicionales.
- Misión del sistema. En sistemas de misiones críticas no se debe de depender de un solo fabricante. Evitaremos estar sujetos a las decisiones del fabricante.

Además de los citados, otro factor a tener en cuenta en el diseño de un sistema IoT y en la evaluación de las tecnologías a utilizar, es la comunicación. En IoT, el consumo de energía es una de las cuestiones dominantes, ya que esta es necesaria para poder transmitir y recibir mensajes y representa el mayor consumo de la energía total necesaria en el dispositivo. Los aspectos a considerar son los siguientes:

- Distancia entre el emisor y el receptor.
- Naturaleza de los obstáculos.
- Distorsión del ruido.
- Regulaciones gubernamentales.

Basándonos en estos aspectos, tendremos que elegir las tecnologías y protocolos adecuados a cada escenario. En el caso de que solo necesitemos comunicarnos dentro de un edificio, podemos utilizar Zigbee o WiFi, dependiendo del tamaño del mismo, mientras que si hablamos de Smart Citys, o aplicaciones en las que las distancias entre dispositivos son del orden de decenas de kilómetros, elegiremos Sigfox o Lora o cualquier otra tecnología LPWA.

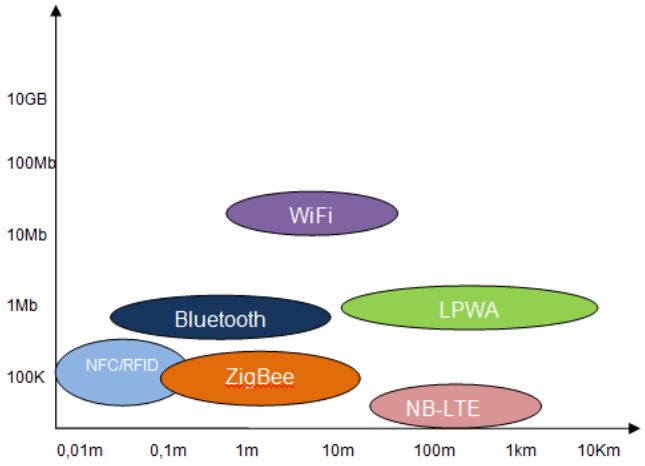


Ilustración 37: Tasa de datos y alcance

5. Aplicaciones IoT

Internet supuso una revolución que trajo consigo la simplificación de múltiples procesos, la expansión de la comunicación personal ubicua y accesible, a la vez que estableció las bases de una fuente de conocimiento y almacenamiento de datos hasta entonces inimaginable.

IoT, supone un avance para estrechar el espacio existente entre el usuario y la máquina, al impulsar la comunicación entre máquinas y sistemas que cooperan entre sí, realimentando y evolucionando proactivamente los procesos y permitiendo un control sobre nuestro entorno cada vez más efectivo.

Todo esto se materializa en una nueva ola tecnológica, con nuevos dispositivos servicios y aplicaciones, que marcará el crecimiento socioeconómico durante los próximos años.

IoT va a cambiar nuestro día a día, mediante dispositivos que se conectan entre sí y a la red. La información sobre nuestro entorno estará disponible de forma accesible y en tiempo real, de forma que pueda enriquecer nuestra experiencia y facilitar la actividad cotidiana, mediante aplicaciones y servicios que pueden ir desde la optimización del uso energético hasta aplicaciones de seguridad, salud, ciudades inteligentes….

Mediante dispositivos conectados, las ciudades crearán ecosistemas que podrán ser empleados para el desarrollo de aplicaciones que mejoren los procesos típicos de la ciudad y permitirán ofrecer a los ciudadanos información en tiempo real.

5.1. Áreas de aplicación.

Las posibilidades de aplicación de IoT son muy variadas, abarcando diversos campos de actividad. IoT ha evolucionado tanto, que prácticamente abarca cualquier campo de la vida que podamos imaginar. A continuación se describen los que mayor protagonismo y evolución están alcanzando.

5.1.1. Smart Home.

Uno de los campo de aplicación en el que se han desarrollado mas proyectos es el de las Smart Home o casas inteligentes. Sensores de temperatura, actuadores para apertura y cierre de persianas, electrodomésticos inteligentes que avisan de la caducidad de los alimentos y son capaces de realizar pedidos cuando alguna existencia alcanza un determinado nivel.

Ilustración 38: Smart Home

IoT abre un amplio abanico de posibilidades para el desarrollo de aplicaciones creativas. Un frigorífico inteligente que compra alimentos en línea, proporcione información nutricional de los alimentos. El frigorífico sabe lo que tiene dentro gracias a los sensores de presión de las repisas y a las etiquetas RFID que disponen los recipientes. Un altavoz avisa de las calorías del alimento retirado, también puede avisar que esta semana está por encima del peso, ya que se ha conectado con la balanza del baño y ha consultado los datos de su peso. IoT, permite conectar objetos que aparentemente no tienen relación para crear una nueva funcionalidad.

En una Smart Home los sensores son los encargados de dar información de la casa. Cada habitación necesita aportar una determinada información que consiste en: temperatura, presencia, estado de ventanas, persianas y puertas y cualquier otra necesaria. En este tipo de entornos es donde el uso de distintas tecnologías de comunicación, de corto alcance (bluetooth, zigbee) para recogida de datos de los dispositivos y de largo alcance (LPWA) para el transporte de estos datos a la nube, se hace más patente y donde el desarrollo de estándares deben de permitir que diferentes tecnologías puedan interactuar entre sí.

5.1.2. Smart City.

Las Smart Citys, o ciudades inteligentes, son aquellas ciudades que aplican las tecnologías de la información y de la comunicación (TIC) para proveerlas de infraestructuras que garanticen:

- El desarrollo sostenible.
- El incremento de la calidad de vida.
- La mayor eficacia de los recursos disponibles.
- Fomentar la participación ciudadana activa.

Ilustración 39: Smart City

En definitiva, se trata de ciudades sostenibles económica, social y medioambientalmente. Las ciudades inteligentes nacen de la necesidad de mantener una armonía entre estos aspectos.

Smart City es otro campo en el que IoT está muy presente, a través de dispositivos que recopilan la mayor cantidad de datos para facilitar la vida al ciudadano. Las aplicaciones pueden ir desde el Smart Parking, indicando

donde existe aparcamiento libre, o indicar que una plaza de minusválido está siendo ocupada por un vehículo no autorizado, el Smart Traffic para informar, tiempo real, del tráfico y proponer rutas alternativas, gestión eficiente del alumbrado.... Estos son solo unos ejemplos de lo que se pretende implementar con esta tecnología, su futuro es muy prometedor sobre todo viendo como muchas comunidades y empresas están apostando claramente por convertir las ciudades en un ecosistema más inteligente y conectado.

Un ejemplo ilustrativo de Smart City, lo representa la ciudad de Barcelona, que dispone del proyecto CityOS. Su principal objetivo es crear un sistema operativo virtualizado para todos los dispositivos y servicios ofrecidos en la ciudad. Barcelona se ha centrado principalmente en smart transportation y smart water. El primero se implementa utilizando una red de sensores con análisis centralizado y smart traffic lights.

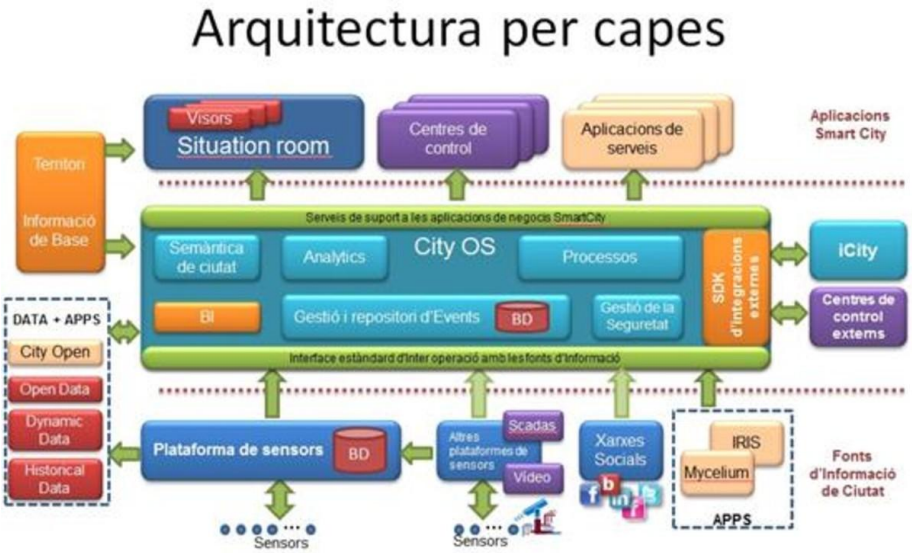


Ilustración 40: City OS

Esta iniciativa ha apostado por la tecnología de Sigfox, al adjudicar a la UTE compuesta por Cellnex Telecom, Accenture y el Grupo ENGIE, un contrato de 30 meses para impulsar el desarrollo de CityOS.

De forma similar Barcelona posee sensores en la mayoría de sus, drenajes, tanques y líneas de suministro de agua. Esta información se integra con información meteorológica y de utilización, dando lugar a un plan estratégico centralizado, permitiendo a la ciudad estimar las necesidades de agua para uso domestico e industrial.

5.1.3. Agricultura y ganadería.

La agricultura tradicional ha aplicado durante años las mismas herramientas y procesos. El sector agrícola se ha percatado del gran potencial que las tecnologías de vanguardia tienen para facilitar el trabajo diario, reducir pérdidas o mejorar el rendimiento y la calidad del producto. A pesar de que a la agricultura le está costando arrancar en este medio, probablemente por ser un área en el que la evolución tecnológica nunca ha sido una prioridad, si que se está intentando revolucionar la forma en la que trabajan los agricultores. Obtener información en tiempo real de diferentes parámetros

de agua, suelo o aire de cualquier campo permite tomar decisiones estratégicas para ahorrar recursos y optimizar los rendimientos. Las aplicaciones, en esta área van desde la toma de decisiones, controlar automáticamente riego, protección de heladas, fertilización. La agricultura inteligente se convertirá en el campo de aplicación más importante en los países predominantemente agrícolas.

Ilustración 41: Smart agriculture

Las ventajas para el sector ganadero, son la información periódica sobre la ubicación y el estado del ganado, su estado de nutrición, enfermedades, eficiencia reproductiva, calidad de los pastos… recibiendo en el Smartphone alertas.

5.1.4. Wearables

Un tipo de dispositivos que están tomando gran popularidad son los wearables. Se trata, entre otros, de dispositivos que nos monitorizan durante todo el día determinados parámetros de nuestro cuerpo y entorno más cercano, mostrando esa información en nuestro Smartphone.

Ilustración 42: Wearable technology

Todos estos dispositivos se agrupan en la denominada tecnología vestible (wearable technology), tecnología corporal, ropa tecnológica, ropa inteligente, tecnología llevable o complementos inteligentes.

En la actualidad los dispositivos vestibles pueden categorizarse de la siguiente manera:

- Salud.
- Deporte y bienestar.
- Entretenimiento.
- Industrial.
- Militar.

5.1.5. Industrial IoT.

IIoT consiste en el uso de tecnologías de IoT en la manufactura de productos, o en la industria en general. Se trata de una tendencia importante con implicaciones significativas para la economía global. Incorpora, además de las propias e IoT, tecnologías de machine learning y big data.

Se trata de una tendencia emergente y todavía no existe ninguna plataforma que domine el sector, de momento las posibilidades de IIoT se basan en:

- Computación basada en sensores.

Gestión de datos en tiempo real, para fabricantes, servicios públicos y minería. Plataformas de recolección de datos de sensores y control de procesos para la mejora del rendimiento, ahorro de energía…

- Analítica industrial.

Información analítica para evitar el tiempo de inactividad del equipamiento, optimizar los beneficios y gestionar los riesgos.

- Aplicaciones inteligentes.

Desarrollo ágil de aplicaciones para productos conectados.

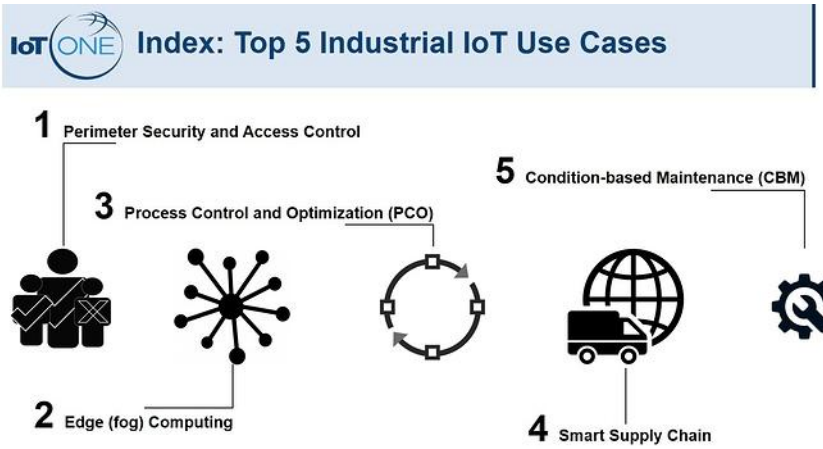


Ilustración 43: IIoT

5.2. Consideraciones de diseño.

Las soluciones IoT, en su gran mayoría están formadas por componentes, cada uno de estos componentes deben de incorporar medidas de seguridad para permitir la protección contra diferentes vulnerabilidades. Estos componentes se ejecutan en tres niveles distintos:

- Nivel de Dispositivos/Gateways:

  En este nivel se protege contra elementos maliciosos que pretenden adquirir los datos enviados por los dispositivos.

- Nivel de Red/Transporte:

  La protección contra dispositivos que envían datos falsos con el objetivo de corromper los datos persistentes de la aplicación.

- Nivel de aplicaciones:

  En el nivel de aplicación la protección se centra en evitar el uso inválido de los datos o la manipulación de los procesos que los analizan dentro de la aplicación.

Es precisamente en este nivel donde los dispositivos IoT exponen a los posibles atacantes la mayor superficie de ataque. El nivel de aplicación incluye todos los dispositivos que tengan conectividad con los dispositivos IoT incluyendo además aplicaciones, tanto locales, las basadas en la nube y las móviles.

En el desarrollo de aplicaciones para IoT, una parte intrínseca del ciclo de vida de desarrollo es la seguridad, en las etapas de diseño, desarrollo y pruebas.

En la etapa de planificación o diseño de la aplicación, se debe de realizar una evaluación formal de los requerimientos de seguridad y privacidad.

Para todas las aplicaciones del IoT la seguridad de las aplicaciones debe ser una parte intrínseca del ciclo de la vida del desarrollo de las aplicaciones (SDLC), particularmente durante las etapas de diseño, desarrollo y pruebas. Dentro de la etapa de planificación o diseño de una aplicación IoT, debe haber una evaluación formal "de arriba hacia abajo" de los requisitos de seguridad y privacidad de la aplicación planificada.

La siguiente tabla describe brevemente cada nivel y las consideraciones de seguridad en las que se deben enfocar los desarrolladores.

Nivel	Descripción	Consideraciones
Aplicación	Despliegue de aplicaciones IoT	• Seguridad de la aplicación • Llamada API segura. • Seguridad de Node-RED • descifrado de mensajes • Mensaje de verificación de checksum
Red/Transporte	Plataforma de mensajería IoT	• Autenticando dispositivos (sólo pueden enviar datos los dispositivos confiables) • Autorización • Seguridad de la API • Configuración de seguridad • Transporte seguro
Dispositivos/Gateways	Los dispositivos (directamente o a través de gateways) publican los datos del sensor y reciben las instrucciones para ejecutar las funciones de control.	• Autenticación • Cifrado del mensaje de carga • Suministro y verificación de certificados • Transporte seguro • Arranque seguro • Firewalls • Actualizaciones de firmware y parches

Ilustración 44: Consideraciones de seguridad

Estas consideraciones de seguridad son fundamentales para el diseño y desarrollo de aplicaciones para IoT, donde todo lo que se puede fabricar, puede considerarse un candidato para la conectividad. Añadiendo características que proporcionan a los usuarios acceso directo o remoto a información proporcionada por diferentes dispositivos.

A menudo los desarrolladores dudan en adoptar nuevas tecnologías debido a que su falta de experiencia alargue el ciclo de vida de diseño del producto.

Las aplicaciones IoT, se alejan del paradigma tradicional de desarrollo, por lo que presenta una dificultad adquirir la experiencia necesaria para llevar a cabo todas las etapas necesarias para desarrollar un producto IoT. Es de vital importancia comprender completamente los diferentes requisitos hardware, software y de certificación, necesarios para el diseño de la aplicación. Será necesario tener en los siguientes aspectos:

5.2.1. Objetivo de la aplicación.

Es necesario entender el escenario de uso, para poder determinar los niveles de potencia y rendimiento necesarios. Diferentes escenarios necesitaran requerimientos diferentes, rastrear productos en una cadena de

suministro, monitorización del desgaste, proporcionar datos en tiempo real, automatización y control…

5.2.2. Tamaño.

Los dispositivos son del menor tamaño posible, el rendimiento generalmente está limitado por el tamaño permitiendo la transmisión de pequeñas cantidades de datos. Los requisitos de tamaño y rendimiento marcan la necesidad de una batería de larga duración para satisfacer las demandas de consumo de energía, lo que puede hacer que la solución general sea más grande y más costosa.

El equipamiento en un gran espacio en un edificio puede ser igualmente difícil ya que tendrá que determinar cuántos componentes serán necesarios para garantizar la transmisión de la señal suficiente en toda una instalación.

5.2.3. Requisitos de comunicación.

En interiores o zonas urbanas, donde tecnologías WiFi y otras tecnologías inalámbricas están disponibles sin mucha dificultad, el alcance puede medirse en metros o decenas de metros. En campo abierto o rural, el alcance necesario para que la señal llegue a la estación radio más cercana podría ser kilómetros, lo que necesitará de tecnologías que permitan estas distancias (LPWA, LTE-M).

Si la ubicación es remota de difícil acceso, la duración de la batería será importante. Las interferencias con otros dispositivos de radiofrecuencia y obstáculos físicos también pueden afectar la distancia operativa.

5.2.4. Fuente de energía.

La energía transmitida es un punto crítico en el diseño de una aplicación ya que afecta tanto a la distancia como a la vida de la batería. A mayor distancia mayor energía necesaria, lo que implica una menor duración de la batería para dispositivos alimentados de esta forma. Por lo tanto todas las consideraciones de diseño deben de focalizarse en el ahorro de energía. La elección de la tecnología de red debe de ajustarse al consumo de energía, la frecuencia con la que los dispositivos se comunican, ya sea entre sí o con servidores/gateways, ha de diseñarse de forma óptima para reducir el consumo de energía.

5.2.5. Consideraciones ambientales.

La verificación de que sistemas inalámbricos son capaces de operar en situaciones específicas (caliente, frio, húmedo, seco) y situaciones extremas es importante ya que necesitarán de monitorización frecuente e incorporar alertas de emergencia basadas en determinados umbrales permitidos.

5.2.6. Comunicación con otros productos.

En un entorno abierto y heterogéneo con diferentes productos y fabricantes, la interoperabilidad es importante, y va más allá del cumplimiento de organizaciones de estandarización ya que puede ocurrir que incluso estándares bien conocidos se interpreten de más de una forma. Por ejemplo si dos fabricantes de controladores de acceso al medio (MAC), compatibles con 802.11b, pero uno no incluye toda la funcionalidad para una operación

específica, aunque ambos son compatibles con el estándar, pueden no ser compatibles entre sí o con una aplicación.

Para garantizar la interoperabilidad es necesario realizar un proceso de certificación de pruebas y de interoperabilidad.

5.3. El impacto del internet de las cosas en nuestra sociedad.

Con IoT, será posible que todo, personas y dispositivos, estén conectados durante todo el tiempo, recibiendo y procesando información. Como resultado aparecerán nuevas formas de toma de decisiones, respaldadas por la disponibilidad de información.

Esta disponibilidad de información en todo momento ha propiciado que surja una nueva generación de consumidores, que demandan productos y servicios basados en la ubicuidad y la conectividad. Estos cambios productivos y en los hábitos de los consumidores han producido cambios en las relaciones entre todos los agentes involucrados.

Desde el punto de vista social y económico, tres aspectos de IoT pueden destacarse:

- El impacto directo sobre las personas.
- La tendencia a modelos de negocio cada vez más abiertos y colaborativos.
- La optimización de las cosas.

5.3.1. El impacto directo sobre las personas.

El término ubicuo hace referencia a una realidad que traspasa los límites del tiempo y espacio, haciendo que lo digital y real se diluyan para permitir que la informática se integre en el entorno de la persona. Por otro lado la expresión “en cualquier lugar” representa un estado en el que todos nosotros y las cosas que nos importan pueden estar conectados a través de una red global lo suficientemente fluida, amplia y segura. La experta del Future Trends Forum, Emily Green [30] utiliza la expresión anywhere (en español en cualquier lugar) que da título a su libro.

Cada día importa menos donde estamos para poder estar conectados, ya que de la posibilidad de conexión dependerá de si puede estar localizado o no. La localización aporta un mayor valor a la información que generamos junto con los objetos que nos rodean, gracias a la ubicuidad de la red.

Una nueva generación de consumidores ha surgido en paralelo con la banda ancha móvil que espera estar conectado permanentemente para que la red le facilite todas las actividades que desea llevar a cabo. ¿Me das la clave de la WiFi?, es una pregunta que se hace en cualquier lugar, para asegurarse la conexión al mundo.

Desde el punto de vista empresarial, los fabricantes, en muchos casos reinventan objetos existentes, extendiendo sus capacidades con conectividad a la red. Un bote de pastillas con conexión a Internet para llevar el control de las dosis.

En definitiva, el desarrollo del Internet de las Cosas está llevando a que el consumidor sea cada vez más exigente. Estar más conectados y localizables facilita una mayor personalización de los servicios y objetos que

nos rodean, así como una mayor información disponible en el momento de la toma de decisiones.

5.3.2. Hacia un nuevo modelo de negocio más colaborativo.

La irrupción de IoT, está dando lugar a nuevos modelos abiertos de colaboración, similares al del open source en el mundo del software.

Google, se ha centrado en la venta de servicios, ofreciendo todos sus productos de forma gratuita, captando a usuarios que no quieren pagar por utilizar sus aplicaciones durante periodos cortos de tiempo. Estas quedan obsoletas o son sometidas a mejoras por los propios usuarios rápidamente. El open source es un movimiento que se centra en que al compartir el código fuente, las mejoras que pueden aportar terceras personas dan como resultado un producto infinitamente mejor. Hay que recordar que Linux principal competidor de Windows y precursor de otros sistemas operativos nació, continuando en la actualidad, como un proyecto de código abierto.

El apoyo, que empresas consolidadas, han prestado al desarrollo del open source, están desplazando los modelos tradicionales de negocio a otros modelos más abiertos y colaborativos.

Las formas de negocio deben de ser capaces de cambiar para adaptarse, sin que esta adaptación impacte de forma negativa sobre las funciones centrales, añadiendo valor a la cadena de valor de la empresa. Los desarrolladores son capaces de diferenciar las partes que cambian frecuentemente de las que permanecen iguales. En este sentido SOA (service oriented architecture) aísla las funciones de negocio en servicios independientes que no cambian con frecuencia.

La gran mayoría de las empresas están subiéndose al tren de las redes sociales, para acercarse al consumidor y descubrir nuevas líneas de negocio. El smart business lleva la interacción en la red al extremo, de manera que el negocio no presenta ninguna jerarquía y se autogestiona mediante la colaboración de personas motivadas (Wikipedia).

ABB, líder global en tecnologías electrotécnicas y de automatización, explora la idea de crear comunidades de dispositivos colaboradores conectando dispositivos inteligentes a una red social (SIoT). Estos personificarán a un sistema que interactuará con los usuarios finales para generar contenidos de valor para una comunidad, interactuando con usuarios finales y expertos técnicos. A través de de la conectividad utilizada para proporcionar servicios remotos, estos dispositivos permitirían que los problemas se resuelvan de forma ágil y precisa. Además, los diagnósticos son capturados y fácilmente reutilizables.

Esta tendencia a planteamientos cada vez más abiertos y colaborativos demuestra que los incentivos económicos no siempre están detrás de los nuevos modelos de negocio. La innovación colaborativa tiene el potencial de ir más allá de nuevos productos y servicios para descubrir, diseñar y desarrollar sistemas ubicuos en los que la innovación prime ante todo.

No obstante lo anterior, una nueva forma de negocio se ha abierto para las operadoras de telecomunicaciones, tanto para nuevos operadores como para operadores ya consolidados, ya sea ofreciendo nuevos servicios de

interconexión de miles de dispositivos o bien desarrollando nuevas tecnologías para aprovechar la infraestructura disponible sin interferir en los servicios que actualmente ofrecen.

6. Conclusiones.

Internet de las cosas se está introduciendo rápidamente en nuestra vida cotidiana proporcionando calidad de vida mediante la conexión de dispositivos, tecnologías y aplicaciones. La automatización y conexión de todo lo que nos rodea requiere de una serie de tecnologías, protocolos y aplicaciones que son la base de sustento de IoT.

La arquitectura, los diferentes componentes y protocolos que constituyen IoT, necesitan de una visión global, que permitan por un lado comprender los diferentes aspectos de este nuevo paradigma y a su vez permitir abordar algunos de los desafíos y problemas relacionados con las tecnologías, su diseño y el despliegue de IoT.

Una de los aspectos a tener en cuenta es el desarrollo de nuevas tecnologías de comunicación que permitan la comunicación de decenas de miles de dispositivos con limitaciones de consumo de energía a grandes distancias. El desarrollo de estas ha abierto nuevos mercados e impulsado el desarrollo de otras tecnologías, por parte de otros actores ya consolidados, para obtener cuota de mercado y aprovechar la infraestructura existente.

En las capas más bajas de la arquitectura, las tecnologías se encuentran en un estado de desarrollo muy avanzado, no obstante hay mucho mas por desarrollar en el resto de capas, desarrollo que impactará en la vida humana de formas insospechadas en las próximas décadas.

7. Glosario.

3GPP 3rd Generation Mobile System.
AMQP advanced message queuing protocol
CoAP constrainded application protocol
DDS data distribution service.
GSM Global system for mobile communications.
GSMA Global system for mobile communications association.
HTTP hypertext transfer protocol.
IETF Internet engineering task force.
IoT internet of things.
ISM Industrial, Scientific and Medical
LoRa long range
LoRaWAN log range wide area network.
LPWA-LPWAN low power wide area-low power wide area network.
LTE long term evolution.
M2M machine to machine.
MQTT message queue telemetry transport.
NB-IoT Narrow band internet of things.
NFC near field communication.
OSI open system interconect.
OGC Open Geospatial Consortium
RFID radio frequency identification.
SC-FDMA single carrier frequency división multiple access.
SDO standards development organizations
XMPP extensible messaging and presence protocol.

8. Bibliografía

[1] O. Vermesan, P. Friess, P. Guillemin et al., “Internet of things strategic research roadmap,” in Internet of Things: Global Technological and Societal Trends, vol. 1, pp. 9–52, 2011.

[2] I. Peña-López, Itu Internet Report 2005: The Internet of Things,2005.

[3] IEEE Internet Initiative,Towards a definition of the Internet of Things (IoT),

Issue 1 – Published 13 MAY 2015.

[4] Peter Mell and Tim Grance. The NIST definition of cloud computing. National Institute of Standards and Technology,

[5] Alessio Botta, Walter de Donato, Valerio Persico, and Antonio Pescap_e. On the integration of cloud computing and internet of things. In Future Internet of Things and Cloud (FiCloud), 2014 International Conference on, pages 23{30. IEEE, 2014.

[6] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli, Fog Computing and Its Role in the Internet of Things

[7] http://social-iot.org. 12/03/2017

[8] Luigi Atzori, Antonio Iera, Giacomo Morabito, and Michele Nitti, The Social Internet of Things (SIoT), When Social Networks meet the Internet of Things: Concept, Architecture and Network Characterization, Computer Networks, Volume 56 ,Issue 16, 14 November 2012, Pages 3594-3608.

[9]Joan Borrell Viader, Jordi Casas Roma, Carles Garrigues, Màrius Montón, Cristina Pérez Solà,Xavier Perramon Tornil, Helena Rifà, Sergi Robles Martínez, Tecnologías de la smart city, Oberta UOC Publishing, SL, Barcelona 2016.

[10] http://coap.technology, 25/03/2017.

[11] http://mqtt.org/ 26/03/2017.

[12] https://xmpp.org/ 26/03/2017.

[13] https://www.amqp.org 27/03/2017.

[14] http://portals.omg.org/dds/ 28/03/2017.

[15] Keith E. Nolan, Wael Guibene, Mark Y. Kelly, An Evaluation Of Low Power Wide Area Network Technologies For The Internet Of Things, Intel Labs Europe, Intel, Leixlip, Dublin, Ireland.

[16] Minh-Tien DO, Claire GOURSAUD , and Jean-Marie GORCE, On the Benefits of Random FDMA Schemes in Ultra Narrow Band Networks, Centre of Innovation in Telecommunications and Integration of service, INSA-Lyon, Lyon, F-69621, France Sigfox Wireless, Batiment E-volution, 425 rue Jean Rostand, Labège, F-31670, France

[17] https://www.sigfox.com

[18] Leverege 2017, LPWAN White Paper

[19] Augustin, A.; Yi, J.; Clausen, T.; Townsley, W.M. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. Sensors 2016, 16, 1466.

[20] An Ultra-Wide Band System with Chirp Spread Spectrum Transmission Technique Peng Zhang, Hao Liu National Key Laboratory of Communications University of Electronic Science and Technology of China Cheng Du, Sichuan 610054 P.R. China.

[21] Principles of spread-spectrum communication systems. Don torrieri, Springer,Boston,2005.

[22] Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melià-Seguí, Thomas Watteyne, Understanding the Limits of LoRaWAN, IEEE Communications Magazine January 2017

[23] https://www.cellnextelecom.com,

[24] https://www.vodafone.es.

[25] GSMA: 3GPP Low Power Wide Area Technologies.

[26] http://www.businessinsider.com/verizon-launches-national-iot-network-2017-4, 10/04/2017

[27] Y.-P. Eric Wang , Xingqin Lin , Ansuman Adhikary , Asbjörn Grövlen , Yutao Sui , Yufei Blankenship , Johan Bergman , and Hazhir S. Razaghi, A Primer on 3GPP Narrowband Internet of Things (NB-IoT).

[28] http://www.3gpp.org/news-events/3gpp-news/1628-rel13

[29] Wael Guibene, Keith E. Nolan, Mark Y. Kelly, Survey on Clean Slate Celular-IoT Standard Proposals, Intel Labs Europe, Intel, Leixlip, Dublin, Ireland.

[30] Michael Marcovici, The Internet of Things.

[31] Emily Nagle Green, Anywhere: How Global Connectivity is Revolutionizing the Way We Do Business, Copyrigth 2010 by Yankee Group Research Inc.