Dar las gracias a todas las personas que me han ayudado en esta etapa universitaria. A todas las personas que han creído en mí, aun cuando yo no lo he hecho.

A Macarena Espinilla Estévez, mi tutora, por ayudarme y estar siempre a mi disposición.

Una y mil veces gracias.

ÍNDICE

1 INTRODUCCIÓN

1.1 Motivación

El presente proyecto tiene como objetivo estudiar y evaluar las aplicaciones del paradigma de Iot en el Transporte Terrestre. El Internet de las cosas (Iot), se considera como la relación que existe entre ellos, que se conectan a una Red (Internet) y ofrecen datos a tiempo real. También se puede considerar como la digitalización del mundo físico. En la mayoría de los casos el Iot, facilita las actividades diarias del ser humano.

(Sanz, 2017)

1.2 Estructura

El presente trabajo está estructurado en tres grandes bloques:

- El primero, este presente, en el que se hace una introducción al TFM y explicación de la realización de él.
- El segundo, en el que se estudia el Internet de las Cosas desde su origen hasta la actualidad, pasando por la tecnología que se requiere para este gran fenómeno de la tecnología.
- Y por último, un tercer bloque en que se trata de temas del Internet de las Cosas pero mas enfocado a la logística y al transporte.

1.3 Justificación

Este trabajo se realiza y se redacta por Iván Lerma Villar, que es supervisado por la profesora Doña Macarena Espinilla Estévez. La realización de este trabajo es a petición de la Escuela Politécnica Superior de Linares (EPSL) para poder finalizar el Máster de Ingeniería del Transporte Terrestre y Logística. El Trabajo Fin de Máster (en adelante TFM), cumple con las directrices de la Normativa sobre Trabajos Fin de Máster por la Universidad de Jaén y sigue las normas básicas de estructura, estilo y redacción que se detallan en el documento “Normas básicas de estilo y estructura para la elaboración del TFM”, elaboradas y aproadas por la Comisión de TFM de la Escuela Politécnica Superior de Linares.

2 INTERNET DE LAS COSAS (INTERNET OF THINGS)

2.1 Origen del Internet de las Cosas

(Cendón, 2017) El termino Internet de las Cosas, se enmarca en el siglo XIX debido a los primeros experimentos de la telemetría de la historia. El primero de estos experimentos fue de la mano de los técnicos franceses, los cuales desarrollaron unos dispositivos que permitían obtener información meteorológica y también permitían conocer el espesor de nieve. Estos dispositivos se colocaron en la cima de la montaña Mont Blanc. A través de enlaces de radio de onda corta, los datos eran transmitidos a la Sede de París.

La idea del Internet de las Cosas, el poder conectar objetos entre sí ya lo tuvieron en cuenta Nikola Tesla o Alan Turing, pero debido a la falta de los avances en la tecnología y en la investigación, fue la consecuencia de que todo se quedara en “entelequias imposibles de realizar”.

Fue a mitad de los años 60 principio de los 70, cunado se desarrolló los primeros postulados de comunicación, que han ido evolucionando hasta dar a lugar a lo que hoy en día se conoce como Internet. Todo esto se realizó dentro de la red ARPANET, del departamento de Defensa de los EE. UU.

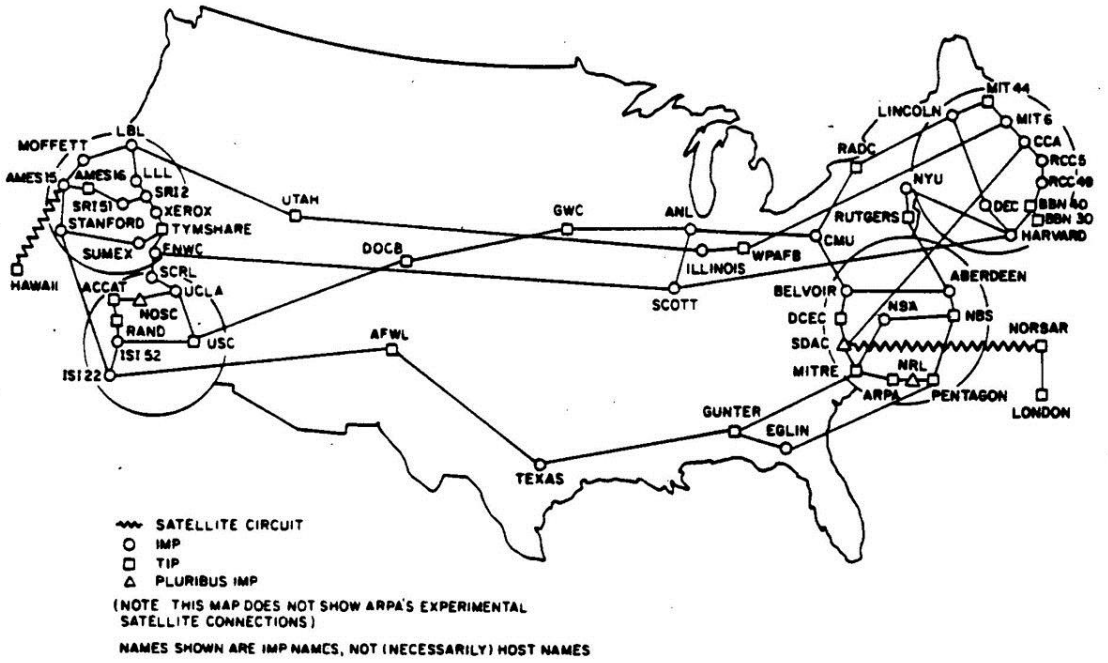

Figura 1. Red ARPANET en 1977.

A finales del Siglo XX, en el año 1990, John Romke, inventó el primer objeto conectado a Internet, una tostadora que se podía encender o apagar en remoto. Pero no ha sido hasta el actual siglo, Siglo XXI, cuando se ha producido la revolución de los objetos conectados a Internet, debido a la demanda de la conectividad inalámbrica a Internet, esto ha originado que surjan nuevos conceptos como son: Wireless Sensor Networks (WSN) o Machine to Machine (M2M), para llegar a lo que se conoce como Internet de las Cosas (Iot).

2.2 Evolución del Internet de las Cosas

Aunque el concepto de Internet de las Cosas (IoT) es un concepto relativamente nuevo, su origen data de hace 40 años. En la actualidad, se pueden identificar tres fases de evolución del IoT:

- La primera fase se refiere a la tecnología embebida, es decir, ordenadores integrados en dispositivos a los que se accedía a sus datos mediante controladores. Como puede ser los cajeros automáticos de las sucursales bacarias.

- La segunda fase aparece con la masificación de la conectividad y el cloud computing, es decir diferentes dispositivos conectados que toman y envían información desde la nube. Ejemplo: Creación del Ordenador portátil.

- La tercera fase tiene lugar en la actualidad y agrega inteligencia a los datos, con Big Data y herramientas de analítica.

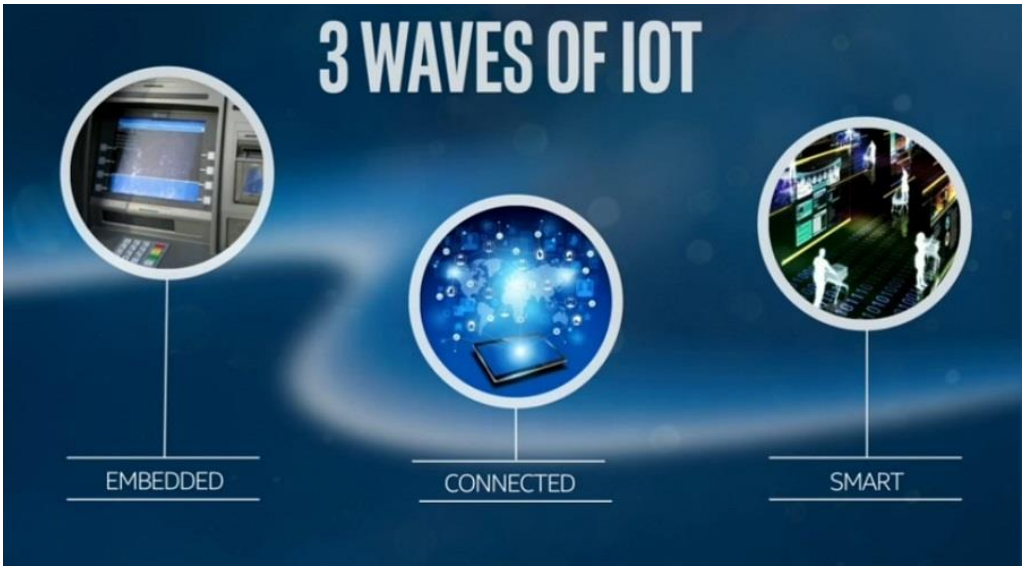

Figura 2. Evolución del Internet de las Cosas.

El fin de esta evolución, de la tercera etapa, es mejorar la producción de productos y ofrecer servicios inteligentes, incluso antes que los requieran los usuarios.

El Internet de las Cosas no solo debe de mejorar la vida de las personas, sino que también debe de impactar positivamente en:

- Cuidado a una población cada vez más longeva.
- Cambio climático
- Administrar el crecimiento de las ciudades.
- Producción y distribución de alimentos.

2.3 Introducción al Internet de las Cosas

Con la llegada del Internet de las Cosas, se prevé que la vida de los seres humanos esté llena de máquinas que se conecten a Internet, que se comunicaran unas con las otras, a través de Internet sin la necesidad de que el humano intervenga en esa comunicación. A esto se le llama: comunicación máquina a máquina, M2M, (machine to machine).

Esta comunicación, M2M, es imprescindible para las aplicaciones de la ciudad inteligente (Smart City), en la que podemos encontrar aplicaciones como: el transporte inteligente, casas inteligentes, aparcamiento inteligente, peaje inteligente, conducción inteligente, en definitiva, todas aquellas aplicaciones que ayudan a facilitar el día a día de las personas en la ciudad.

Según el artículo científico, Technologies and challenges in developing Machine-to-Machine applications: A survey, "*la interoperabilidad es un gran desafío en el desarrollo de aplicaciones M2M, porque los dispositivos son producidos por varios proveedores y la falta de estandarización hace que sea extremadamente difícil permitir la interacción entre los dispositivos*". (Anum, Ghalib A, Muhammad, & Usam, 2017)

En definitiva, el concepto Internet de las Cosas, se refiere a la revolución en las relaciones entre los objetos convencionales y las personas e incluso entre los propios objetos. En otras palabras, se trata de la digitalización del mundo físico, o lo que es lo mismo, que todos los utensilios tradicionales se conecten con la red y también se sincronicen entre ellos mismos para ofrecer un servicio mucho más pleno y eficiente. De este modo, esta idea pretende potenciar objetos que años atrás se conectaban mediante un circuito cerrado, lo hagan ahora globalmente mediante el uso de la red de redes para interactuar entre ellos. (Polo, 2015)

Un claro ejemplo de Iot, sería que, al sonar el despertador, la cafetera empezara a hacer café, es decir una especie de "acción-reacción" pero entre aparatos. Aun así, el Iot no es algo reciente. Desde hace más de dos décadas, aproximadamente, diversos sectores

trabajan en la idea de hacer lo más interactivo posible todos los objetos de uso cotidiano para así poder alcanzar lo que se conoce como el hogar inteligente (Smart House) o también poder alcanzar las ciudades inteligentes (Smart City).

Figura 3. Smart House.

Figura 4. Smart City.

El funcionamiento del Internet de las Cosas (Polo, 2015) se debe mediante un hardware especializado, lo que los expertos llaman “sistemas embebidos”, que permite a los objetos conectarse no solo a Internet, sino también programar eventos o llevar a cabo órdenes que se le haya mandado o dictado de forma remota. Es decir, son chips y circuitos que ofrecen la posibilidad de cumplir una serie de tareas muy específicas, las cuales serán asignadas según su dirección IP, ya que todos los objetos tendrán una IP específica y se podrá acceder a cada uno de ellos para asignarle una tarea. Aunque también se podría contactar con un servidor externo y enviar los datos que recoja.

Para entender este concepto tan abstracto, se muestra algunos ejemplos:

- La nevera podría indicarnos la fecha de caducidad de los alimentos que están a punto de rebasarla.
- Otro ejemplo, sería que nuestro cepillo de dientes nos informara si ha detectado alguna caries y en caso de ser así, pidiese cita en nuestro dentista.
- Otro caso el retrete podría tomar nuestras muestras de orina y avisarnos de los valores que estuvieran alterados.

Según fuentes consultadas, como es el caso de la página: “*what news”,* estima que para el 2020, habrá casi 50.000 millones de dispositivos, aproximadamente, estarán preparados para conectarse a Internet con el objetivo de proporcionar una serie de servicios a la sociedad y aplicaciones inteligentes sin precedentes. Algunas compañías, como es el caso de Samsung, han presentado el prototipo “SleepSense”, que controla, entiende y mejora el sueño de las personas. Otra compañía, como LG, presenta “Smart ThinQ”, es un sensor que permite conectarse con los electrodomésticos y conocer, por ejemplo, si la lavadora ha terminado de hacer el centrifugado.

Pero innovaciones de esta gran envergadura, como es el Iot, tiene algunos inconvenientes, como puede ser la pérdida de privacidad, ya que se estará cediendo constantemente nuestras vidas más aún a la tecnología, que podría llegar a ser hackeada como en la actualidad y poner en peligro nuestra información personal. Otro inconveniente, es que cualquiera podría llegar a tomar el control de nuestro hogar. Tal vez, estos inconvenientes y el alto coste de los sistemas sean algunos motivos por los cuales el Iot no se ha asentado en nuestra sociedad en su totalidad, pero es cuestión de tiempo.

2.4 Smart City: Mobility

(Logitek, 2013) Es más que evidente, que, desde el Siglo pasado, Siglo XX, las ciudades han tenido un gran desarrollo, este desarrollo se ha basado en fomentar el uso del automóvil propio, lo que ha causado un aumento en los índices de contaminación, no

solo en la contaminación atmosférica, debido al aumento de los niveles de CO_2, sino también al aumento del ruido, contaminación acústica, debido que hay más coches.

Estos ejemplos son síntomas de una cuidad no inteligente, las Smart City o Ciudades Inteligentes, basadas en la movilidad, se caracterizan por:

1. Utilizar sensores que permitan a los elementos de tráfico estar integrados en un único mando de control.
2. Tener acceso a lo que ocurre en la ciudad o estar viendo lo que ocurre en tiempos real.
3. Priorización de los medios de transporte público, sanitarios y de emergencias, a través de los análisis del flujo del tráfico de la ciudad.
4. Detectar de manera automática las infracciones cometidas en la vía o accidentes que se hayan producido.
5. Sensores para las plazas de aparcamiento y así poder gestionar de una mejor manera la demanda.
6. Sistemas capaces de establecer comunicación entre infraestructura, vehículo y usuario, todo esto a tiempo real.
7. Sistemas automatizados para la red de transporte público.
8. Sistemas de mantenimiento y diagnóstico.

Lo anteriormente mencionado, son las características que presente una red de movilidad urbana de una Smart City. Pero, ¿Cuáles son las ventajas que se pueden conseguir al aplicar el concepto de Smart City?

1. Se aumenta la seguridad vial.
2. Aumento de la accesibilidad a la ciudad.
3. Disminución del uso del automóvil propio.
4. Reducción de la contaminación.
5. Mejor optimización de los servicios del transporte público.
6. Se disminuye las congestiones de tráfico.

2.5 Smart Environment

Un entorno inteligente es, de acuerdo con Mark Weiser, "*un mundo físico que está ricamente entretejido e invisible con sensores, actuadores, visualizadores y elementos computacionales, integrados a la perfección en los objetos cotidianos de nuestras vidas, y que conectados a través de una red continua*".

Cook y Das, definen el entorno inteligente como: *"un pequeño mundo donde los diferentes tipos de dispositivos inteligentes están constantemente trabajando para hacer más cómoda la vida de los habitantes".*

El Smart Environment Systems, lo que pretende es reducir y facilitar a las personas los trabajos de gran esfuerzo, trabajos peligrosos, o trabajos en los que siempre se actúan de la misma forma, con el objetivo de mejorar la calidad de vida de las personas.

Los entornos inteligentes se clasifican ampliamente para tener las siguientes características:

- Control remoto de dispositivos, como sistemas de comunicación de línea de alimentación para controlar dispositivos.
- Comunicación del dispositivo, utilizando middleware y comunicación inalámbrica para formar una imagen de los entornos conectados.
- Adquisición / diseminación de información de redes de sensores.
- Servicios mejorados por dispositivos inteligentes.
- Capacidades predictivas y de toma de decisiones.

2.6 Smart Water

El objetivo del Smart Water es el control y el uso razonado del agua. Este es un aspecto básico que contempla las Smart Cities.

- Grifos inteligentes, con el objetivo de evitar desperdicios innecesarios de agua.
- Análisis inteligente de la calidad del agua en las depuradoras de las ciudades.
- Medición de nivel y caudal en ríos y canales, a través de sensores.
- Evitar inundaciones en las presas.

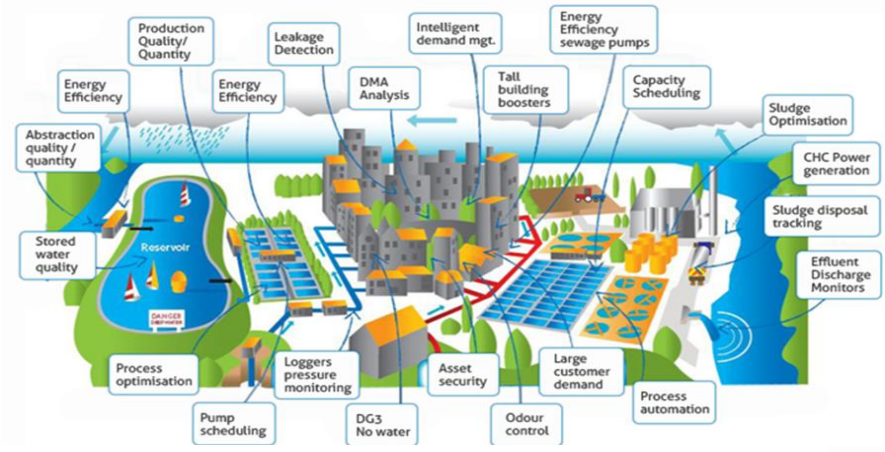

Figura 5. Smart Water.

2.7 Logística

(Logística, 2018) Según el estudio realizado por *Zebra Technologies Corporation,* más del 90% de las empresas dedicadas al sector del transporte y la logística consideran que el Iot supondrá un impacto beneficioso, ya que permite a las empresas adaptar sus productos a la producción y el diseño según la demanda del mercado.

La empresa, ICP Logística, dedicada a la logística, ha creado una patente, que está desarrollando, que consiste en el packaging inteligente, el cual permite, a través de sensores, enviar y recibir información del estado en el que se encuentra cada uno de sus paquetes y/o envíos, todo esto a tiempo real.

Para poder llevar esto acabo, se utilizan unos sensores que tienen que ser capaces de:

- Geolocalizar el pedido en el mapa a tiempo real.
- Conocer la temperatura del producto a través de termómetros, esta función es de especial interés para productos que deben de tener una determinada temperatura y así evitar romper la cadena de frio durante el transporte, por ejemplo: productos alimenticios, productos farmacéuticos, etc.
- También deben de ser capaces de identificar la humedad a la que está expuesta la mercancía, para así evitar problemas de que se moje la mercancía y por consiguientes pueda llevar a su deterioro. Esto es uno de los problemas a lo que se enfrentan las empresas dedicadas al transporte de mercancías debido al mal estado en el que se puede encontrar el recubrimiento del tráiler encargado de realizar el transporte. Gracias a estos testigos de humedad se podría resolver problemas de este tipo.
- Sensores de movimientos y golpes, este tipo de sensores ayudarán a detectar posibles daños que pueda sufrir el producto.

Esta patente permitirá mantener informado al cliente en todo momento del estado en el que se encuentra la mercancía y poder responder, de manera inmediata, en caso de accidente o emergencia.

Figura 6. Internet de las Cosas en Logística.

2.8 Agricultura Inteligente

La agricultura inteligente consiste básicamente en modernizar el campo a través del Internet, en otras palabras: aplicar la tecnología a la agricultura.

Aplicando las nuevas tecnologías en el mundo rural, podemos conseguir beneficios que desde hace algunos años ya se están experimentando en otros ámbitos más ligados a la ciudad.

El objetivo es aumentar el rendimiento de las instalaciones agropecuarias incrementando notablemente su producción y reduciendo costes.

Una herramienta principal es la agricultura de precisión que se basa en conocer, de manera, exacta las necesidades de los cultivos y actuar sobre ellos de forma proporcionada, es decir, sin gastar más recursos de los necesarios ni quedarse cortos.

También permite realizar tratamientos de herbicidas y fertilizantes más eficientes ahorrando dinero, tiempo y productos.

Una apliacion en este sector es AgroLocation Intelligence, que consiste en el análisis y visualización de los datos Agro. La georreferenciación de los datos permite ser mucho más precisos y eficientes.

2.9 Domótica y Automatización del hogar

Se llama domótica a los sistemas capaces de automatizar una vivienda o edificación de cualquier tipo, aportando servicios de gestión energética, seguridad, bienestar y comunicación, y que pueden estar integrados por medio de redes interiores y exteriores de comunicación, cableadas o inalámbricas, y cuyo control goza de cierta ubicuidad, desde dentro y fuera del hogar. Se podría definir como la integración de la tecnología en el diseño inteligente de un recinto cerrado.

La automatización de edificios es el control centralizado automático de los sistemas de calefacción, ventilación y aire acondicionado, iluminación y otros de un edificio mediante un sistema de gestión de edificios o un sistema de automatización de edificios (BAS). Los objetivos de la automatización de edificios son la mejora de la comodidad de los ocupantes, la operación eficiente de los sistemas de construcción, la reducción en el consumo de energía y los costos operativos, y el ciclo de vida útil mejorado de los servicios públicos.

La automatización de edificios es un ejemplo de un sistema de control distribuido: la red informática de dispositivos electrónicos diseñados para monitorear y controlar la seguridad mecánica, de seguridad contra incendios e inundaciones, iluminación (especialmente iluminación de emergencia), HVAC y control de humedad y sistemas de ventilación en un edificio.

La funcionalidad básica de BAS mantiene el clima dentro de un rango específico, proporciona luz a las habitaciones según un calendario de ocupación, monitorea el rendimiento y las fallas de los dispositivos en todos los sistemas y proporciona alarmas de mal funcionamiento al personal de mantenimiento del edificio. Un BAS debería reducir los costos de energía y mantenimiento del edificio en comparación con un edificio no controlado.

(Wikipedia, 2018)

Según el artículo “Sistema de gestión de edificios”: el término sistema de automatización de edificios, poco utilizado, se refiere a cualquier sistema de control eléctrico que se utiliza para controlar un sistema de calefacción, ventilación y aire acondicionado (HVAC). El BAS moderno también puede controlar la iluminación interior y exterior, así como la seguridad, las alarmas contra incendios y básicamente todo lo demás que es eléctrico en el edificio. Los viejos sistemas de control HVAC, como los termostatos

con cable de 24 V CC o los controles neumáticos, son una forma de automatización, pero carecen de la flexibilidad e integración de los sistemas modernos.

2.10 eHealth

Hace referencia a la práctica de cuidados sanitarios apoyada en tecnologías de la información y las comunicaciones (TIC).

Que el sistema sanitario utilice el Internet de las cosas, puede facilitar en:

- Prevención de enfermedades.
- Personalización del sistema sanitario.
- Seguridad del paciente aumenta.
- Seguimiento de indicadores del estado de salud y registro metódico de datos e informes del estado de salud del paciente.
- Gestión telemática de servicios de salud a través de Internet.

2.11 Wearables

Son dispositivos electrónicos que se conectan a Internet y son de consumo diario. En los últimos años ha aumentado su demanda y por lo tanto su comercialización. Como puede ser el aso de relojes que se conectan con nuestro teléfono móvil, pulseras que indica las calorías gastadas en función de los pasos que realiza en usuario. Pulseras que indican las pulsaciones de nuestra frecuencia cardiaca. (Software, 2016)

Figura 7. Wearables.

2.12 Aspectos legales a tener en cuenta en Iot

Todos los dispositivos que utilizan Internet para poder ofrecer un servicio pueden crear ciertas dudas de seguridad, debido a que utilizan y manejan datos e información de la vida cotidiana de los usuarios.

Pero no solo se pueden crear ciertas dudas de seguridad en los usuarios, también los dispositivos conectados a Internet tienen que garantizar el derecho a la competencia, es decir asegurar la privacidad entre grandes empresas.

(Asesoría, 2017) En lo referente a la protección y propiedad de datos, existe el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo: "protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, que armonizará, a partir de 2018, el marco de la UE para el tratamiento de datos personales".*

El Reglamento anteriormente citado, garantiza a los usuarios, un correcto uso de sus datos personales también garantiza a las empresas el correcto funcionamiento de un único mercado digital.

(Asesoría, 2017) *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016*: *"asegura que los datos de las víctimas, testigos y sospechosos de la comisión de delitos se encuentren debidamente protegidos en el ámbito de una investigación criminal o de aplicación de la ley".*

Directiva 2013/40/UE: "ataques contra los sistemas de información y por la que se establecen normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información". (Asesoría, 2017)

La Directiva 2013/40/UE protege de la cibercriminalidad.

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016: "relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, cuyo objetivo es establecer un nivel común de ciberseguridad en toda la UE y mejorar la coordinación de los Estados Miembros ante posibles ataques cibernéticos". (Asesoría, 2017). En general de lo que trata la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, es sobre la ciberseguridad.

Directiva 2014/53/UE: "armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos dictada en materia de estandarización". (Asesoría, 2017)

Ley 15/2007, de 3 de julio, de Defensa de la Competencia. Debido a esta Ley, puede ser que se den casos en los que, dispositivos electrónicos de diferente marca no puedan conectarse entre sí.

2.13 Seguridad

Los ordenadores personales o los smartphones actúan de una manera general, es decir, pueden realizar varias funciones y no realizan una función específica. Gracias a que los ordenadores y los smartphones son capaces de realizar varias funciones, son más difíciles de ser amenazados ante un ciberataque o un hackeo, aunque esto no significa que estén exentos de ello.

Pero en el caso del Internet de las Cosas, los dispositivos pueden sufrir posibles amenazas debido a que el fabricante, es el encargado del diseño y del mantenimiento del software, lo que hace que estos dispositivos sean más vulnerables.

En el caso de los ordenadores y de los smartphones, utilizan un sistema operativo en común (Windows, Linux...) y se pueden obtener actualizaciones de seguridad.

Cabe destacar el concepto de seguridad por defecto en Inglés: “Security by Default”. La seguridad por defecto, en el software, significa que los por defecto las opciones de configuración son las más seguras configuraciones posibles, que no son necesariamente los más de uso fácil configuración. En muchos casos, la seguridad y la facilidad de uso se evalúan según el análisis de riesgos y las pruebas de usabilidad. Esto lleva a la discusión de cuáles son los ajustes más seguros en realidad. Como resultado, el significado preciso de "seguro por defecto" permanece indefinido.

Otro punto añadido, es la geolocalización de los dispositivos, debido a que los dispositivos conectados al IoT, tienen como objetivo satisfacer y mejorar la vida de las personas, deben de situarse en sitios frecuentados por personas, o lo que es lo mismo, zonas muy concurridas. Todo esto, más la accesibilidad de los dispositivos, los hacen más vulnerables y puede ser la principal causa de amenazas para los dispositivos conectados a IoT.

2.13.1 Deficiencias de la seguridad en la transmisión de datos

Una vez llegados a este apartado nos centraremos en las amenazas o deficiencias que se puede producir en un ataque relacionado con la transmisión de datos, dado que estos dispositivos están continuamente enviando información entre dispositivos o a Internet. Una de las medidas fundamentales será la protección de la información en el tránsito de la información.

Es fácil comprender la importancia de la seguridad en las comunicaciones para este tipo de dispositivos. Todas estas comunicaciones, especialmente las que se propagan por

medios inalámbricos o por redes públicas son sensibles de sufrir ataques a la confidencialidad en las comunicaciones.

Cuando los dispositivos o implementaciones no garanticen un nivel aceptable de seguridad en la identificación, privacidad, e integridad en las comunicaciones realizadas, es muy probable que estas deficiencias puedan ser aprovechadas por un atacante remoto para comprometer la información intercambiada. Esta información puede incluir datos privados o de carácter personal, o bien puede tratarse de datos técnicos que se puedan emplear para realizar otro tipo de ataques que, por ejemplo, faciliten el control del dispositivo.

Si no se protege adecuadamente el canal de comunicación mediante el cifrado de datos, puede ser sencillo para un intruso realizar ataques de tipo Man In The Middle. Este tipo de ataques se basan en que el atacante puede capturar el tráfico del cliente, rectificarlo para aparentar ser él el originador del mismo y remitirlo al servidor legítimo, de modo que actúa como un punto intermedio en las comunicaciones, invisible tanto para el origen como para el destino del tráfico. Así puede obtener toda la información que desee incluso modificarla para alterar el comportamiento o funcionamiento de cualquiera de los dos extremos.

2.13.2 Deficiencias en la seguridad de la plataforma Software

El aprovechamiento de vulnerabilidades de software es una de las amenazas más comunes en estos dispositivos conectados a Internet.

En cierto tipo de dispositivos se utilizan versiones ajustadas de sistemas operativos de uso común (Windows XP, Android, Línux, etc.) de forma que se abaratan los costes de fabricación. Este hecho, evidentemente, supone un riesgo de seguridad, ya que cuando se detectan vulnerabilidades sobre dichas plataformas son explotables sobre todos los dispositivos que las instalan, facilitando a los potenciales atacantes una puerta de entrada para infinidad de dispositivos.

Otro vector de ataque incluso más habitual que el anterior son las interfaces web, de uso muy frecuente en dispositivos IoT, ya que éstos normalmente son de tamaño reducido y no disponen de monitor, teclado o dispositivos apuntadores, permitiendo su administración desde otro dispositivo habilitado.

Otra característica común a una gran cantidad de dispositivos es el uso de servicios en la nube. En este caso dichas aplicaciones suponen otro vector de ataque, ya que si existen deficiencias en la gestión o actualización de este tipo de plataformas se podrá acceder a la información que puedan almacenar; así como dependiendo del servicio que se preste, incluso tomar el control del dispositivo IoT. En algunos dispositivos como las

Smart TV se pueden descargar e instalar aplicaciones de terceros sobre el propio dispositivo que amplían su funcionalidad, al igual que sucede con los smartphones, las cuales normalmente se obtienen de repositorios de aplicaciones o markets que mantienen los propios fabricantes. En estos casos se pueden emplear estas aplicaciones como puerta de entrada para tomar el control del dispositivo, así como para obtener información. Este tipo de ataque se puede perpetrar de dos formas posibles; la primera sería explotando vulnerabilidades identificadas en el software, y la segunda podría ser descargando aplicaciones maliciosas, bien sea desde una fuente oficial que no analice suficientemente la seguridad de las aplicaciones que incorpora, o bien desde un canal no oficial de aplicaciones.

Por último, está muy de moda emplear aplicaciones móviles que se instalan en nuestro smartphone para cualquier tipo de gestión, bien sea obtener datos o controlar el dispositivo. Debido a ello, las aplicaciones móviles también pueden ser objetivo de ataques, ya sea aprovechando vulnerabilidades o deficiencias en su implementación, o mediante el desarrollo de aplicaciones maliciosas que emulen el comportamiento y aspecto de las legítimas para obtener acceso a los dispositivos IoT.

2.13.3 Deficiencias en la seguridad de la configuración y funcionalidad

Otro punto fundamental en la seguridad de cualquier sistema es su propia funcionalidad. En muchas ocasiones, bien los desarrolladores (configuración por defecto) o los propios usuarios no mantienen un criterio alineado con la seguridad en la implementación o configuración de la funcionalidad de un servicio. En este aspecto, el panorama en el mundo de IoT es semejante, ya que la mayoría de los dispositivos no siguen una política adecuada de SbD.

Como consecuencia de este hecho, la mayoría de los dispositivos habilitan muchas de sus funcionalidades en sus configuraciones por defecto, normalmente muchas más de las que emplea el usuario. Hay que ser conscientes de que cada uno de estos servicios habilitados pueden suponer una brecha de seguridad en la actualidad o en un futuro si no se actualizan o gestionan adecuadamente.

2.13.4 Deficiencias en la seguridad del hardware

Los ataques contra hardware se basan fundamentalmente en entender la estructura y realizar un análisis de comportamiento del dispositivo a atacar, basándose en sus capacidades. Se emplean este tipo de ataques cuando la seguridad software es robusta o en sistemas localizados en redes aisladas o bien protegidas de un acceso público vía Internet.

Cabe destacar que, para realizar este tipo de ataques, se suele requerir el uso de equipamiento especializado. Dependiendo del equipo que se disponga se podrán realizar distintos tipos de ataque desde monitorización de interfaces hasta ingeniería inversa y manipulación de componentes internos.

La aplicación de medidas de seguridad dependerá en gran medida de la criticidad del dispositivo considerada por el fabricante, su uso previsto y la criticidad de los datos que gestione.

Una técnica de ataque habitual en este aspecto es el acceso directo a componentes de almacenamiento tanto volátil (memoria) como no volátil (disco duro, memoria flash). De este modo, dependiendo del diseño del dispositivo será más o menos sencillo el acceso a memoria, así como dependiendo de si dispone de las protecciones implementadas en los datos será fácil acceder a la información en disco del mismo.

2.13.5 Deficiencias en la seguridad de los usuarios

El principal ataque que se puede llevar a cabo es la denominada Ingeniería Social (Social Engineering). Se basa en una manipulación psicológica de los usuarios, empleándolos como vía de acceso a los sistemas mediante acciones de engaño o estafa. Empleándola, los atacantes se aprovechan del desconocimiento o la ignorancia para obtener la información necesaria para alcanzar su fin.

Dado que la mayoría de los sistemas y servicios en la red se protegen mediante el uso de nombres de usuario y contraseñas, el objetivo habitual es intentar obtener este tipo de credenciales mediante estafas por cualquier vía, habitualmente correo electrónico. La mayoría conocemos casos de phishing, que normalmente se envían de forma masiva y poco personalizada, centrados en la obtención de credenciales de acceso a servicios de correo electrónico o acceso a banca online. Sin embargo, cuando se trata de un ataque algo más elaborado es habitual realizar una investigación previa de la víctima en Internet consultando fuentes públicas, realizando actividades de recolección de información. Cuanto más descuidada o incauta sea la víctima al publicar o facilitar su información en la red, más fácil le resultará al atacante perpetrar un ataque más preciso, y en consecuencia con una mayor probabilidad de éxito.

2.14 Tecnologías utilizadas en Internet de las Cosas

2.14.1 Tecnología basada en la recolección de datos

Este es el dispositivo más visible de cualquier sistema IoT. Funciona principalmente o como un dispositivo de detección para reunir información del entorno físico o como un actuador para controlar el mundo exterior con una salida. En algunos casos, los dispositivos

periféricos realizan un papel doble actuando tanto como dispositivos de detección como como actuadores para recopilar y controlar el entorno físico.

El nodo periférico debe estar conectado a la red externa, ya sea mediante un nodo de detección (WSN) con cable o inalámbrico.

Un dispositivo de nodo periférico ofrece la inteligencia para detectar, medir, interpretar y conectar una puerta de enlace de Internet a la nube. Es posible procesar previamente los datos con alguna forma de análisis antes de transmitirlos para lograr una mayor profundidad en la inteligencia de la extracción de los datos.

Las aplicaciones IoT más grandes requieren un gran conjunto de dispositivos periféricos para conformar una red. En esos casos, los dispositivos (nodos) periféricos necesitan un identificador único para que sea posible reconocerlos y comunicarse con ellos de forma efectiva.

Ejemplos típicos de los dispositivos (nodos) periféricos incluyen:

Sensores: de temperatura, humedad, presión, gas, luz, sonido, RFID, NFC, ultrasónicos, medidores de flujo, de fluidos, cámaras, etc.

Actuadores: interruptores, relés, controladores lógicos programables, motores, luz, sonido, etc.

(Element14, 2016)

2.14.2 Tecnología basada en la comunicación de datos

(Soltanmohammadi, Ghavami, & Naraghi, 2016)

En los dispositivos conectados a Internet, la red que se utiliza para la transmisión de datos es la red inalámbrica, que ofrece las siguientes ventajas:

- Ubicuidad. Acceso móvil a la información desde cualquier lugar de su área de cobertura.
- Escalabilidad. Despliegue con diversas topologías y fácil incorporación de nuevos usuarios.

A su vez, también presentan los siguientes inconvenientes:

- Interferencias electromagnéticas. Usan bandas de frecuencias de libre acceso o espectro compartido.
- Seguridad limitada. Posibilidad de acceso por usuarios no autorizados.

El sistema de transmisión inalámbrico más generalizado es la red WiFi. Se trata de una red digital multiservicio para transmitir información de cualquier tipo (voz, datos y video) bajo protocolo IP.

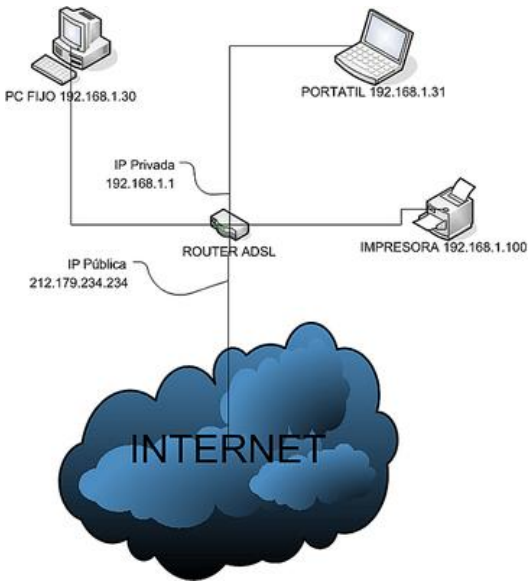

Figura 8. Protocolo IP.

Existen diversas categorías de redes inalámbricas, en función de su rango o alcance:

- PAN (Personal Area Network). Redes para interconexión de dispositivos personales (PDAs, portátiles, tablets) a muy corto alcance (< 10m), baja velocidad (< 1Mbps) y visión sin obstáculos. Ejemplo: Bluetoot (IEEE 802.15).
- LAN (Local Area Network). Redes de interconexión corporativa (oficinas, escuelas, etc.) con cobertura de entorno a 150 m y veloidades entre 2 y 54 Mbps Ejemplo: WiFi (IEEE 802.11).
- MAN (Metropolitan Area Network). Redes usadas para interconexión de distintas oficinas de una empresa en el radio de una ciudad (< 50Km). Pueden alcanzar velocidades de hasta 150 Mbps. Ejemplo: WiMAX fija (IEEE 802.16).
- WAN (Wide Area Network). Conjunto de redes interconectadas con u área de cobertura < 150 Kms y velocidades entre 10 y 384 Mbps. Ejemplo: WiMAX móvil (IEEE 802.20).

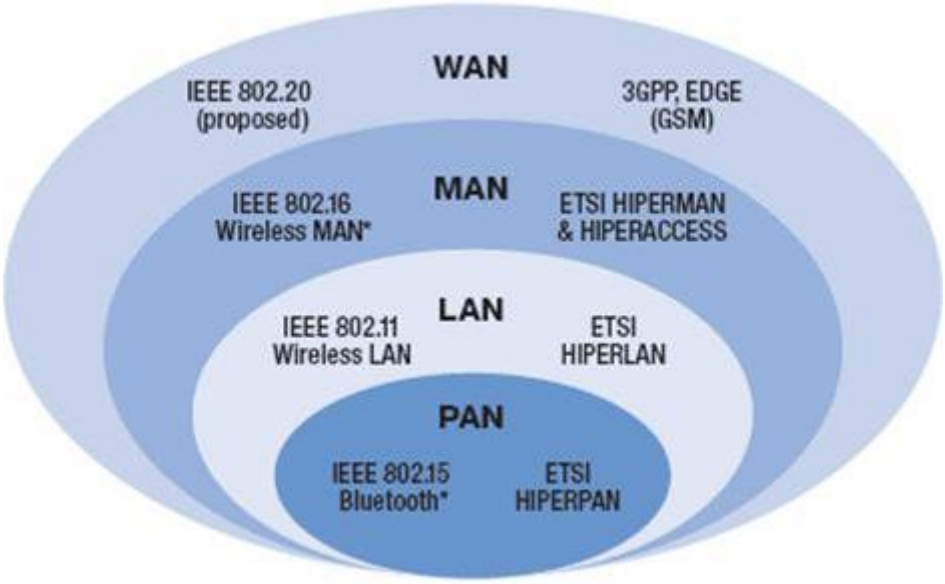

Figura 9. Global Wireless Standards.

2.14.3 Tecnología basada en el almacenamiento y análisis

Otra de las tecnologías usadas en el Iot, es la tecnología que se encarga del almacenamiento, caducidad, análisis y propiedad de los datos de personas físicas y/o entidades, los cuales deben de tener un seguimiento continuo, con el fin de poder actualizarlos de forma eficaz. Este proceso se lleva a cabo en la plataforma denominada BigData.

BigData hace referencia al conjunto de todos los datos, de gran volumen, originados por dispositivos. (Software, 2016)

3 INTERNET DE LAS COSAS EN EL TRANSPORTE

El internet de las cosas supone un gran cambio en nuestras vidas, debido a las grandes ventajas que presenta. Del mismo modo que es un gran avance para nuestras vidas, también lo supone para el sector del transporte y la logística.

La creación de sensores embarcados en las flotas de vehículos (Ibermática, 2018), encargados de realizar el transporte de las mercancías, y la necesidad, por parte de la empresa, de digitalizar toda la información que genera esas flotas, facilitará el trabajo de las empresas dedicadas al transporte, es aquí donde el Iot empezará a funcionar.

El Internet de las cosas, ayudará a las empresas de la logística a tomar decisiones relacionadas con el modo de almacenaje, matización, transporte y entrega, de las mercancías, a los diferentes clientes.

La motorización de las mercancías, se refiere a visualizar en tiempo real, las mercancías para así adelantarse y evitar los posibles problemas relacionados con la entrega a tiempo de dichas mercancías, o problemas relacionados con posibles accidentes en la carretera durante su transporte.

En definitiva, el Internet de las cosas en el sector del transporte y la logística, supone una revolución no solo para las empresas, dedicadas a este sector, si no también para sus clientes, que podrán consultar el estado o dónde se encuentra su mercancía durante toda la cadena de suministro, desde el almacenamiento hasta el transporte y posterior entrega.

Pero el Iot, en el transporte, no solo se aplica al transporte dedicado a lo logística, también se puede aplicar:

- Telepeajes.
- Sensores Inteligentes de Parking.
- Sensores de guiado de parking para detección de plazas ocupadas.
- Comunicación entre coches.

3.1 Sistemas Inteligetes en el Transporte

El concepto de Sistemas Inteligentes de Transporte (SIT) (Inglés: Intelligent Transportation Systems - ITS) es un conjunto de soluciones tecnológicas de las telecomunicaciones y la informática (conocida como telemática) diseñadas para mejorar la operación y seguridad del transporte terrestre, tanto para carreteras urbanas y rurales, como para ferrocarriles.

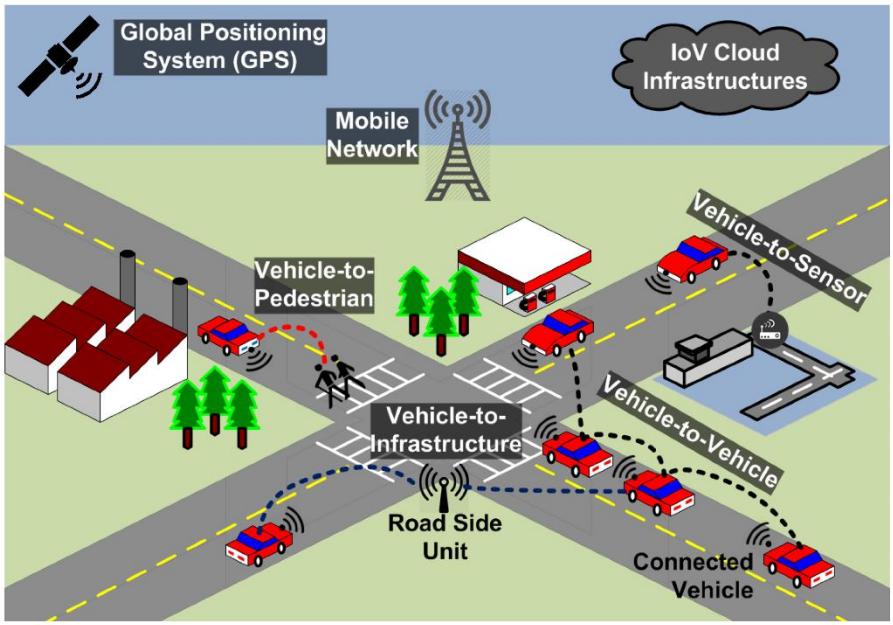

Figura 10. Intelligente Transport Systems.

Existen diversas comunicaciones, en el sistema inteligente del transporte:

- La comunicación entre vehículos **(V2V)** es un conjunto de tecnologías que permiten **el** intercambio de datos entre vehículos, de forma que se puedan llevar a cabo acciones orientadas a mejorar la fluidez en el tráfico, aumentar la seguridad mediante la correcta anticipación de eventos, y comunicarse de forma más eficiente con las fuerzas de seguridad y los servicios de emergencias, entre otras funciones.
- La comunicación entre el vehículo y la Infraestructura **(V2I).** Los avances tecnológicos nos proporcionan ventajas como conductores que antes no se podían ni siquiera soñar. Uno de los avances más notables en el campo de la información hacia el vehículo es el llamado V2I, o lo que es lo mismo, la comunicación entre el vehículo y los elementos de su exterior: otros vehículos e infraestructuras.

3.1.1 Ventajas de utilizar Intelligente Transport Systems (ITS)

1. Aumentan la seguridad en los conductores:

- Seguridad preventiva: El uso de las estaciones meteorológicas permite preveer con bastante precisión las condiciones climatológicas que van a padecer en sus posibles viajes, lo que les va a permitir planificarlos cuando

el tiempo sea el correcto. Estos sistemas, junto con las cámaras de explotación, permiten conocer en cada momento el estado exacto de las carreteras, facilitando la labor de corte de carreteras (cuando las condiciones no son las adecuadas), y de aviso a los conductores de estos elementos.

- Seguridad instantánea: Gracias a los paneles de mensajería implantados en las carreteras, se hace llegar al instante la información de interés que deben conocer los conductores (p.e. fuerte viento, reduzca la velocidad), para tener un viaje más seguro.
- Seguridad reactiva: Para garantizar que los conductores cumplen las normas de tráfico, también se emplean estos sistemas de manera eficaz, con el uso de radares (para el control del exceso de velocidad), o detectores de vehículos que pasan los semáforos en rojo, entre otros sistemas.

2. Mejoran la eficiencia del tráfico: Los sistemas de conteo, que permiten conocer el número de vehículos que pasan por una zona determinada, unido a sistemas inteligentes de rutas utilizadas, permite a los responsables de las carreteras hacer una planificación eficiente de las mismas a medio plazo, que consigan reducir el número de atascos, mejorando el tráfico diario.
3. Permiten llevar un control detallado de los elementos de las carreteras, gracias a sistemas de Inventariado, que garantizan el estado adecuado de todos los elementos (ofreciendo avisos y señales cuando es necesario revisar algún material de la carretera), o los sistemas informáticos que facilitan a los responsables de la explotación de las carreteras gestionar toda la información relacionada con las operaciones de vialidad que se deben realizar, de acuerdo con la carta de servicios.
4. Facilitan la labor de los conductores, por ejemplo habilitando medios para pagar en la autopista sin parar (telepeaje), ofreciendo las mejores rutas a seguir en carretera, o mostrando información detallada al instante sobre las carreteras.

3.1.2 Características

Con el reciente desarrollo de los sistemas inteligentes se pueden tratar problemas de congestión de tráfico y de movilidad urbana en calles y carreteras, puentes, intersecciones, puertos, vías ferroviarias y peajes como parte de la infraestructura del

transporte, elementos que pueden estar interconectados y ser tratados mediante los sistemas inteligentes de transporte con el objeto de mejorar la productividad del sistema, reducir el número de accidentes y reducir las emisiones de efecto invernadero entre otros aspectos. A continuación, se presentan algunas de las características de los sistemas inteligentes de transporte más novedosos utilizados en la actualidad:

1. Sistemas de Información Avanzados de Viajeros, se caracterizan por:

a) Provisión de información de tráfico en tiempo real.
b) Guía de ruta / Sistemas de navegación.
c) Información de estacionamiento.
d) Sistemas de información meteorológica.

2. Sistemas Avanzados de Administración del Transporte:

a) Centros de operación del tráfico.
b) Control adaptable de señales de tránsito.
c) Señales de mensajes dinámicos.

3. Sistemas de tarifas de Transporte Habilitados:

a) Peajes electrónicos.
b) Pago de tarifa o precio electrónico.
c) Líneas de expreso.
d) Tarifas de uso de vehículos por kilómetro recorrido.
e) Variables de las tarifas de estacionamiento.

4. Sistemas de Transporte público Avanzados:

a) Información en tiempo real del estado del sistema de transporte público (por ejemplo: autobús, metro, tren, etc.)
b) Localización automática de vehículos.
c) Pago de tarifa electrónica (por ejemplo, tarjetas inteligentes).

5. Vehículo a Infraestructura de Integración y Vehículo a Vehículo de Integración:

a) Sistema de anticolisión en intersecciones.
b) Adaptación inteligente de la velocidad.

3.1.3 *Nuevas Tecnologías para el control y administración del transporte*

Cada una de las tecnologías implementadas en las redes de sistemas de transporte debe proporcionar información en tiempo real que permita tener control de datos de forma confiable y que facilite su administración; deben brindar información sobre condiciones de tráfico, trabajos de mantenimiento velocidades de circulación, alarmas ante accidentes, entre otras. Dicho proceso de modernización se debe llevar a cabo de forma gradual teniendo en cuenta que debe suplir las necesidades de movilidad en el presente y se debe acomodar igualmente al volumen de tráfico del futuro.

Un ejemplo de esto lo representa la completa gama de soluciones Corning Cable Systems LANscape creada por la empresa líder en soluciones de sistemas de telecomunicaciones, electrónica de consumo y transporte Corning Incorporated, que permiten, diferentes facilidades para la implementación de elementos tecnológicos al sistema de transporte, de tal forma que el proceso se realice en el menor tiempo posible, lo cual evita que exista un tiempo de inactividad en el control y la administración del tránsito. Por otro lado, Siemens una empresa española caracterizada por la innovación tanto tecnológica como en gestión, por medio de su división de negocios denominada “Mobility”, busca mejorar la movilidad minimizando el impacto en el medio ambiente y el presupuesto. En su publicación titulada “Soluciones inteligentes para el tráfico de hoy y del mañana” muestra un esquema de soluciones dependiendo del tipo de tráfico que se presente, el cual se podría resumir a continuación:

TABLA II.
NUEVAS TECNOLOGÍAS PARA CONTROL DE TRÁFICO

Tráfico Interurbano	**Tráfico urbano**	**Parking**	**Sistemas de Túneles**	**Peaje Electrónico**	**Aeropuertos**
Centros de control de Autopistas	Sistemas y centros de control de tráfico	Estaciones de pago	Centros modulares de control de túneles	Sistemas de peaje “Free Flow”	Sistemas de iluminación, mando y presentación.
Sistemas de detección y adquisición de datos de tráfico	Instalaciones de semáforos y controladores de intersecciones	Pago a través de teléfono móvil	Detección de NO_2 CO y falta de visibilidad	Sistema de peaje por satélite	Sistemas de comunicación Tierra/Aire y Tierra/Tierra
Adquisición de datos medioambientales	Sistemas de priorización del tráfico para transporte público de autobuses y tranvías	Sistema de guiado en interior de aparcamiento y en calle	Redireccionamiento de carriles	City Tolling: Zonas de peaje en ciudad basadas en video, DSRC o GPS/GSM.	Sistemas de guiado en pista
Sistemas de llamadas de emergencia	Control del medio ambiente	Sistema de gestión de ocupación de las plazas de aparcamiento	Control de la altura de vehículos, gálibo	Sistemas para recopilación de cobros y cargos.	Sistema de aterrizaje sin visibilidad (G-Bas)
Acceso a información meteorológica		Parquímetros	Tecnología de seguridad y video vigilancia	Sistema de peaje por carriles.	Comunicación Torre de Control

Fuente: SIEMENS, “Soluciones Inteligentes para el tráfico de hoy y del mañana”, pág. 3 [16]

Otros dispositivos empleados son los detectores de lazo que son utilizados en las carreteras para detectar la presencia de vehículos por medio de un lazo inductivo ubicado justo debajo del pavimento. Éstos, junto con los dispositivos de video permiten obtener una cifra exacta del número de vehículos que se encuentran circulando sobre la vía y la velocidad a la que lo hace. Esto hace que sea una herramienta eficaz para la gestión de tráfico pues dichas cifras sirven como base de datos en los centros de control de transporte, permitiendo informar a la comunidad sobre posibles congestionamientos y rutas alternas.

3.2 Telepeajes VIA-T

(VIA-T, 2017) El VIA-T es el Telepeaje instalado en todas las utopistas pertenecientes a la Península Ibérica.

Este tipo de peajes permite al viajero poder pagar la tasa del peaje sin necesidad de bajarse de su vehículo. Para poder usar este tipo de sistemas es necesario que el usuario instale un dispositivo electrónico en el parabrisas del vehículo. (González Barrios, 2014)

Figura 11. Dispositivo VIA-T.

Los vehículos dotados con este tipo de dispositivo pueden circular por las vías de peaje, que admitan este tipo de pago.

En las vías con telepeaje, hay unas antenas con sistemas de comunicación basado en las señales microondas de corte alcance, los datos del dispositivo VIA-T cargan el

importe del peaje de la autopista a su paso por ella. Cuando la antena ha leído correctamente el código, emite un único sonido, el semáforo se pone en verde y por consiguiente la barrera se sube, permitiendo el paso del vehículo. Si, por el contrario, se emite más de un sonido, síntoma de que no ha leído correctamente el código o se ha producido un error, el semáforo se pone en rojo y la barrera no se sube. Para que el sistema sea capaz de leer el código del dispositivo VIA-T, el vehículo debe circular, por el tramo de peaje, a una velocidad comprendida entre 20 km/h y 40 km/h.

Figura 12. Autopista con Telepeaje VIA-T.

3.2.1 Ventajas de utilizar Telepeaje

1. Seguridad y comodidad.

Con este sistema no es necesario disponer de dinero en efectivo, ni si quiera de tarjeta de crédito, tampoco es necesario recoger tickects ni tampoco tener que bajar la ventanilla. Solo basta con tener bien colocado el dispositivo VIA-T y reducir la velocidad a los límites establecidos para que el sistema pueda leer correctamente. De este modo se gana en seguridad, ya que el viajero no tiene que prestar atención nada más que al propio viaje.

2. Rapidez y Fluidez.

No es necesario pararse ya que se trata de un sistema inteligente capaz de leer el código del dispositivo VIA-T, esto supone un ahorro en tiempo y también supone una fluidez en el tráfico debido a que no se tienen que parar los vehículos.

3. Ecológico.

Reducción de gases contaminantes ya que no hay que parar el vehículo.

4. Interoperabilidad.

Este sistema de telepeaje se puede utilizar en todas las autopistas de la Península Ibérica, que dispongan de la posibilidad de telepeaje y también puede ser utilizado por cualquier vehículo.

5. Fiabilidad.

La tecnología utilizada por VIA-T garantiza la seguridad.

3.2.2 Autopistas Españolas con telepeaje

[6] A continuación, se muestran las Autopistas españolas que cuentan con telepeaje:

P-7 - Málaga-Estepona
R-3 - Madrid-Arganda
R-5 - Madrid-Navalcarnero
AP-53 - Santiago - Dozón (Alto de Santo Domingo)
AP-7 - Barcelona-La Jonquera
AP-7 - Montmeló-El Papiol
AP-7 - Barcelona-Tarragona
AP-2 - Zaragoza-Mediterráneo
AP-1 - Burgos-Armiñón
AP-66 - León-Campomanes
C-32 - Castelldefels-El Vendrell (Autopista Pau Casals)
AP-7 - Cartagena-Vera
AP-9 - Ferrol-Frontera portuguesa
AP-9 - Ferrol-Frontera portuguesa
AP-9 - Ferrol-Frontera portuguesa
AP-15 - Tudela-Irurzun
AP-71 - León-Astorga
AP-7 - Tarragona-Valencia
AP-7 - Valencia-Alicante
AP-4 - Sevilla-Cádiz
AP-7-Estepona-Guadiaro
C-16 (E-9) - Sant Cugat-Manresa
AP-7 - Alicante-Cartagena
AG-55 - A Coruña-Carballo

AG-57 - Puxeiros-Baiona

M-12 - Eje Aeropuerto

AP-36 - Ocaña – La Roda

R-4 - Madrid-Ocaña

AP-41 - Madrid-Toledo

AP-68 - Bilbao-Zaragoza

AP-51 - Ávila-Villacastín

AP-61 - Segovia-San Rafael

AP-7 - Circunvalación de Alicante

R-2 - Madrid-Guadalajara

AP-6 - Villalba-Adanero

C-33 - Barcelona-Montmeló

C-32 - Montgat-Palafolls

E-9 / C-16 - Túnel de Vallvidrera

E-9 / C-16 - Túnel del Cadí

E-9 / C-16 - Túnel del Cadí

AP-8 - Ermua-Bilbao

AP-8 - Variante Sur Metropolitana de Bilbao

Túneles de Artxanda

Túneles de Artxanda

Túneles de Artxanda

AP-1 - Álava

AP-1 - Tramo Guipuzcoano

AP-8 - Tramo Guipzcoano

AP-46 - Alto de las Pedrizas-Málaga

Figura 13. Autopistas españolas con telepeaje.

3.3 Sensores inteligentes de Parking

Encontrar aparcamiento en las grandes ciudades o en las ciudades que disponen de poco espacio para tal función. Es uno de los problemas cotidianos con los que se encuentran los ciudadanos de tales ciudades. (Herrador Muñoz, 2013)

Esto supone un aumento de gases contaminantes, debido a las constantes vueltas que tienen que estar haciendo los ciudadanos con sus vehículos. También supone una gran pérdida de tiempo, ya que se emplea mucho tiempo en buscar aparcamiento.

En cuanto a la atención en la conducción, esta se ve reducida debido a que los conductores prestan mayor atención a buscar aparcamiento que a respetar las normas de circulación, suponiendo un riesgo para los demás usuarios de la vía pública.

Para solventar este problema, en algunas grandes ciudades utilizan lo que se llama: Smart Parking. Este sistema consiste en utilizar sensores, instalados en el suelo de la zona donde se puede aparcar. El estacionamiento dotado con estos sensores, manda la información a la “nube” y esta lo manda a todos los dispositivos que tengan conexión a Internet y tengan instalada la aplicación.

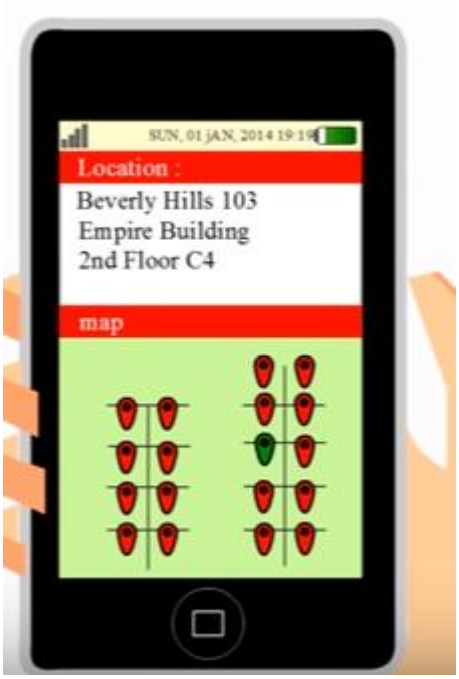

Figura 14. Smart Parking

Dependiendo de si hay algún coche encima del sensor, este mandará una información distinta para que en la aplicación aparezca en color verde, las zonas libres y en color rojo, las zonas ocupadas.

Este concepto, entraría dentro de lo que se conoce como Smart City o Smart Mobility.

3.3.1 Ventajas

El uso del Smart Parking tiene muchas ventajas, (Entel, 2016) no solo para el propio conductor, sino también para el resto de los ciudadanos y demás usuarios de las vías públicas:

1. Ahorrar tiempo, ya que con esta aplicación se va directo al sitio donde se puede aparcar y se evita dar viajes innecesarios.
2. Fluidez en el tráfico, disminuye las posibilidades de congestión del tráfico.
3. Se reduce el estrés en los conductores, muchos aseguran que encontrar aparcamiento puede ser una situación estresante.
4. Se reducen las contaminaciones, no solo de las partículas de CO_2, si no también contaminación acústica.
5. Ahorro económico, se reduce el consumo de combustible.

6. Aumenta la seguridad, tanto para el conductor como para el ciudadano, ya que el conductor se centra en la conducción y así se evitan posibles accidentes.
7. Mejor uso de las áreas, se evita que los vehículos aparquen en zonas de carga y descarga, en zonas para personas con movilidad reducida, paradas de autobuses, de taxis, etc.

3.4 Sensores de guiado de parking para detección de plazas ocupadas

Sensores de guiado de parking para detección de plazas ocupadas están pensado para facilitar el aparcamiento a los usuarios de un parking, reduciendo el tiempo que se tarda desde que entra hasta que aparca, y descongestionando el tráfico que se suele generar para encontrar una plaza libre, reduciendo la polución y el ruido.

La principal ventaja de este modelo de sensor de parking es la unión de dos dispositivos en uno solo. Los sensores ultrasónicos y el indicador LED.

El sensor de parking se instala justo encima de cada plaza de aparcamiento, permitiendo ver la luz LED desde el carril de circulación.

El sensor de parking para detección de plazas funciona mediante la tecnología ultrasónica. Esta tecnología ofrece una gran precisión en la detección en el reconocimiento de un vehículo. Un sensor rápido y con gran fiabilidad, detectando únicamente elementos de grandes dimensiones (vehículos).

El sensor detecta al instante en tiempo real cualquier cambio en el estado de su plaza (vacía o con un vehículo aparcado), modificando el color del indicador LED.

sensor de parking destaca por integrar en el mismo dispositivo los sensores ultrasónicos y el indicador LED de ocupación de la plaza.

El color del LED cambia entre rojo y verde dependiendo del estado de su plaza (libre u ocupada), permitiendo a los conductores reconocer si una plaza está libre u ocupada al momento. También permite indicar plazas para minusválidos con una luz azul.

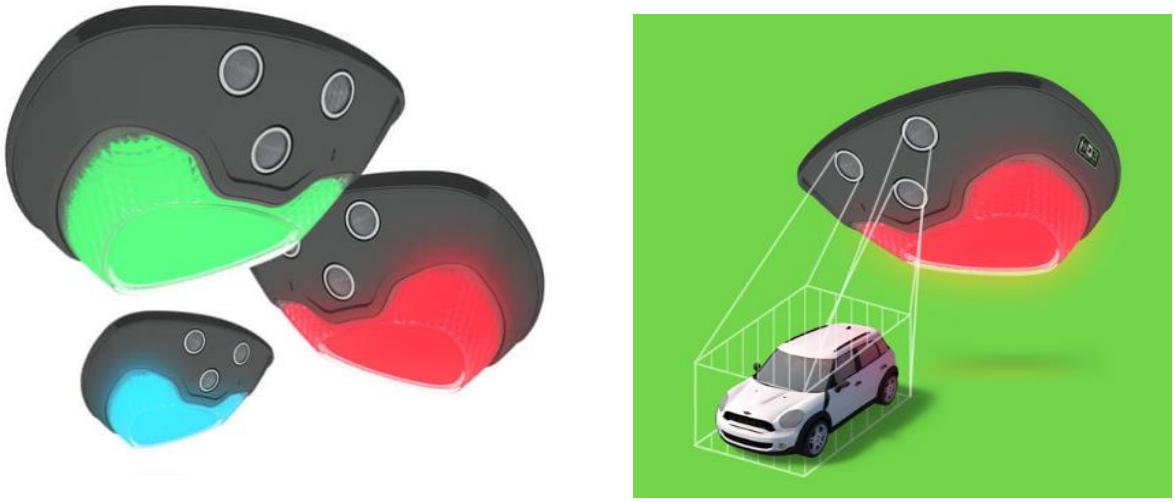

Figura 15. Sensor de Parking.

3.5 Pre- Drive C2X

Pre-Drive C2X intenta crear un automatismo que nos ayude a evitar el efecto acordeón en la carretera. Pre-Drive C2X no es más que una aplicación similar a las de la tecnología C2C, esa que permite que los vehículos se comuniquen entre sí y discutan la jugada en areas de una mayor seguridad y fluidez en la circulación. Este tipo de aplicaciones van a estar presentes cada vez más en nuestros coches, de manera que en unos años serán tan comunes como hoy lo son los principales sistemas electrónicos de seguridad.

Uno de los problemas asociados al efecto acordeón es la sensación de imprevisibilidad por parte del resto de conductores, que de repente se encuentran con la velocidad de los vehículos que tienen delante disminuye, en ocasiones de forma drástica. Bien, pues el sistema Pre-Drive C2X permite avanzar esa información para que el conductor sepa que más adelante se está gestando una retención.

Pongamos un ejemplo: Un coche se ve en la situación de frenar ante un imprevisto en la calzada tiene que frenar hasta los 20 km/h. Los coches que reducen su velocidad por debajo de los 20 km/h envían una señal al resto de los vehículos situados en medio kilómetro a la redonda, de manera que los conductores pueden adaptar la velocidad a la nueva situación. De hecho, es posible programar los coches para que no puedan acelerar más en estas situaciones, pero entiendo que siempre es más deseable dejar esta opción en manos del conductor.

El sistema también prevé la comunicación del coche no sólo con otros vehículos sino con cualquier elemento de la red viaria. De hecho, si las siglas C2C hacen referencia a la comunicación coche a coche (del inglés, car to car), C2X es un sistema de comunicación “coche a lo que sea”; también, al centro de control de Tráfico.

(Camos, 2011)

4 CONCLUSIÓN

5 BIBLIOGRAFÍA

[1] https://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-el-qinternet-de-las-cosasq (Revista muy interesante) (07/03/2018)

[2] Technologies and challenges in developing Machine-to-Machine applications: A survey.

[3] https://wwwhatsnew.com/ (02/04/2018)

[4] https://www.ibermatica365.com/como-impactara-el-internet-de-las-cosas-en-el-transporte/ (28/04/2018)

[5] https://www.icp.es/internet-of-things-llega-a-la-logistica/ (28/04/2018)

[6] http://www.viat.es/ (28/04/2018)

[7] https://www.comunicae.es/nota/pagatelia-inicia-el-servicio-de-telepeaje-con-portugal-1050357/ (28/04/2018)

[8] http://oa.upm.es/21414/1/PFC_DAVID_HERRADOR_MU%C3%91OZ.pdf (29/03/2018)

[9] https://informacioncorporativa.entel.cl/innovacion/smartcities/smartparking (29/03/2018)

[10] http://www.creatingsmartcities.es/ambitossmart-mobility.php (29/03/2018)

[11] http://www.bcendon.com/el-origen-del-iot/ (15/06/2018)

[12] https://www.espacioasesoria.com/Noticias/el-internet-de-las-cosas-iot-y-su-regulacion-legal- (18/06/2018)

[13] http://www.evaluandosoftware.com/campos-de-aplicacion-de-internet-of-things-o-internet-de-las-cosas/ (18/06/2018)

[14] https://www.google.es/search?q=global+wireless+standards&hl=es&gl=es&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj6xvvw_t3bAhUO3qQKHUbwCz4Q_AUICigB#imgrc=3eVvFaGbsdOjuM: (18/06/2018)

[15] http://www.evaluandosoftware.com/tecnologias-aplicaciones-utilizadas-internet-las-cosas/ (18/06/2018)

[16] A survey of Traffic Issues in Machine-to-Machine communications over LTE (20/06/2018)

[17] https://www.theguardian.com/media-network/media-network-blog/2014/jun/20/internet-things-marketing-potential-data (20/06/2018)

[18] http://es.farnell.com/internet-of-things-collect (20/06/2018)

[19] https://imasdetres.com/sensores-guiado-parking/ (20/06/2018)

[20] http://www.circulaseguro.com/pre-drive-c2x-automatismos-contra-el-efecto-acordeon/#more-69925 (20/06/2018)

[21] http://www.circulaseguro.com/tag/car2x/ (20/06/2018)

[22] https://es.wikipedia.org/wiki/Sistemas_inteligentes_de_transporte#Aplicaciones (20/06/2018)

[23] IEEE 802.16e en Intelligent Transport Systems (ITS): https://upcommons.upc.edu/bitstream/handle/2117/10302/802.16e_ITS.pdf?sequence=1&isAllowed=y (20/06/2018)

[24] https://es.wikipedia.org/wiki/Entorno_inteligente (20/06/2018)

[25] https://en.wikipedia.org/wiki/Building_management_system (20/06/2018)

[26] http://www.abc.es/espana/comunidad-valenciana/abci-funciona-smartwater-dispositivo-hara-familias-ahorren-500-euros-agua-201804021340_noticia.html (20/06/2018)

[27] http://smartrural.net/ (20/06/2018)

[28] https://es.wikipedia.org/wiki/ESalud (20/06/2018)

[29] http://catedratelefonica.unex.es/las-tres-fases-de-la-evolucion-de-internet-de-las-cosas/ (20/06/2018)

[30] https://en.wikipedia.org/wiki/Secure_by_default (21/06/2018)

[31] http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf (21/06/2018)

[32] https://www.tecnocarreteras.es/2011/04/11/que-son-los-sistemas-inteligentes-de-transporte-its/ (23/06/2018)

[33] file:///C:/Users/ariad/Desktop/7122-14461-1-SM.pdf (23/06/2018)