EL INTERNET DE LAS COSAS (*INTERNET OF THINGS*, IOT)

Heitor MARTÍNEZ GRUEIRA

(Ing.)

QUISIERA agradecer la oportunidad que se me brinda al permitirme participar en esta serie de artículos técnicos con una tema tan en boga como es el Internet de las Cosas, máxime tras haberme aventurado años atrás únicamente con publicaciones históricas.

Introducción

Hace tan solo unas pocas décadas, internet, tal y como la conocemos hoy día, era un mero sueño tecnológico, muy lejos todavía de hacerse realidad. Actualmente el concepto de equipos interconectados en una red amplia nos es familiar y de uso cotidiano, pero dado que la demanda humana es infinita, igualmente lo es su ansia tecnológica.

Por qué no soñar con un mundo interconectado, donde personas y máquinas interactúen por igual, empleándose los datos que bullen por la red para realizar análisis de tendencias, anticiparse a la demanda, resolver un problema de deslocalización o conocer de primera mano cuáles son los gustos, preferencias o sugerencias reales de la población. Esta vaga idea que por sí misma bien podría parecer ciencia ficción, se ajusta en realidad a un concepto ya acuñado y en plena vigencia, como es el Internet de las Cosas (*Internet of Things*, IoT).

A pesar de lo novedoso que nos pueda ser este concepto, resulta más sorprendente aún si cabe que se trate de algo perfectamente abordable gracias a nuestro desarrollo tecnológico actual. Este concepto versa sobre la idea bási-

ca de interconectar un amplio espectro de objetos mediante internet, que fue planteado en una conferencia impartida en el Instituto Tecnológico de Massachusetts (MIT) en 1999, en la que se abordaban las investigaciones en el campo de la identificación por radiofrecuencia (*Radio Frequency Identification*, RFID) y la tecnología de sensores .

Cuando hablamos de la interconexión de «objetos», en realidad nos estamos refiriendo a la posibilidad de establecer una conexión entre más «cosas u objetos» (o sea, máquinas) que personas. Esta idea básica vislumbra la posibilidad de que ciertos elementos integrantes de la red sean meros equipos que realicen automáticamente procesos de etiquetación, identificación o gestión de dispositivos, como si de humanos se tratase.

La simple ventaja de identificar cualquier clase de objeto (libro, dispositivo, electrodoméstico, paquete, herramienta, etc.) interconectado a través de una red nos permitirá abordar temas de plena actualidad, como pueden ser la logística y su compleja problemática, las rupturas de *stock*, las pérdidas de mercancía por caducidad o extravío, la domótica, etc. Cualquiera de las cuestiones enunciadas será solventada operando sobre el objeto que haya ocasionado la incidencia, tratando de minimizar los efectos adversos. Por ejemplo, si una empresa logística identifica la pérdida de un enlace de paquetería, y dado que su localización o rastreo en la red sería inmediato, siempre que se tratase de un objeto reemplazable podría optarse por emitir un nuevo paquete de manera inmediata al objeto de reducir en la medida de lo posible su demora de entrega, y de tratarse de un objeto irremplazable, organizar su rastreo a partir de la última posición identificada.

Tras consultar diversas estimaciones, las más generosas dictaminan que en el año 2020 podrían alcanzarse los 30.000 millones de dispositivos inalámbricos conectados a internet. Este volumen no es viable mediante el vigente protocolo IPv4, por cuanto será la próxima generación de aplicaciones bajo el IPv6 la que soportará la identificación, tráfico y el procesado de esta gran cantidad de dispositivos interconectados (1).

De acuerdo con la exposición realizada, una infraestructura con las características técnicas y tecnológicas referenciadas estará capacitada para identificar instantáneamente cualquier clase de objeto o dispositivo interconectado a la red. Esta interconexión de dispositivos al IoT es actualmente uno de los campos de investigación tecnológica más amplio y más activo, donde se plantean procedimientos que barajan la idea de emplear señales de radio de baja potencia, prescindiendo de las tecnologías basadas en señales radio *WiFi* o *Bluetooth*.

---

(1) Las capacidades del protocolo IPv6 respecto a su predecesor IPv4 se aportan en el anexo a este artículo.

Tecnologías

Las actuales tecnologías *wireless,* tan extendidas y en plena vigencia, se corresponden con el estándar definido por el Institute of Electrical and Electronics Engineers (IEEE) [802.11x para la red *WiFi* y 802.15x para el *Bluetooth*]. En su momento trataron de responder a las exigencias impuestas por las redes inalámbricas de alto rendimiento, es decir, a los altos volúmenes de señales de transmisión por unidad de tiempo; precisamente por ello, esta tecnología vigente no resultará idónea para el modelo definido de IoT, puesto que no se demandará el tratamiento de grandes volúmenes de datos, ni su emisión a altas velocidades, por lo que no se justifica el elevado consumo de energía que representan.

La infraestructura del IoT se fundamentada principalmente en la interconexión de un número muy elevado de dispositivos que vuelcan en la red un volumen de datos relativamente bajo. Precisamente por ello, tendrá una baja demanda de energía, por lo que actualmente se investiga en el campo de aquellas tecnologías que operan sobre espectros de señal que supongan fuertes ahorros de energía y que además resulten más económicas (*cheap networks*). Entre ellas podemos destacar la *ZigBee* (IEEE 802.15.4, protocolo de red de malla inalámbrica de baja potencia), la RFID y los códigos *Quick Response* (QR) con *touchatag*.

A la vista de lo expuesto, podremos atestiguar sin temor a equivocarnos que el IoT se encuentra todavía en sus primeras etapas de implantación y, por tanto, no es de recibo tratarla como un desarrollo tecnológico real, sino más bien como una innovación que se encuentra todavía en fase de experimentación y cuya verdadera expansión está todavía por llegar. Es importante reseñar que esta nueva filosofía tecnológica no se constriñe a una única topología de red a la que se interconectan diferentes máquinas y dispositivos activos. Por el contrario, este concepto de red tratará el espacio de interconexión de una manera topológicamente independiente, posibilitando la confluencia de datos generados por los distintos dispositivos interconectados, con los que se procederá a su análisis y, en función del resultado obtenido o del conocimiento inferido, se operará en consecuencia sobre ellos.

De esta manera, el IoT representa un proyecto tecnológico de futuro por sí mismo, dirigido esencialmente al mundo industrial y empresarial para crear un nuevo marco de negocio y de estrategias competitivas, las cuales desplazarán el modelo de producción actual y modificarán definitiva e inequívocamente las cadenas de valor del mercado. A la vista de ello, el mercado tendrá que reorganizarse para hacer frente a este nuevo desafío de naturaleza cambiante y en constante evolución.

Finalmente y en consonancia con lo descrito, el IoT se nos presenta como un objetivo en sí mismo, dinámico y cambiante, que será alcanzable únicamente por aquellas organizaciones que trabajen en base al desarrollo de la

propia industria y en función del conocimiento de la demanda real de los consumidores.

Mercado

Uno de los ámbitos que seguramente logrará una mayor expansión y en el que tratarán de inmiscuirse masivamente las empresas será el «hogar inteligente», con el mercado de productos electrónicos de consumo, cuyo ámbito de aplicación no tiene que ver inicialmente con la *domótica*; tratará de crear un espacio donde no solo se evalúe el análisis de situaciones concretas, sino que en función de este será la propia infraestructura la que interopere rápida, consecuente y coordinadamente, con el objetivo ejecutar las acciones definidas o corregir las desviaciones identificadas.

A modo de ejemplo se diseccionan a continuación algunas de las medidas que debería tomar una infraestructura como la descrita al objeto de prevenir los inherentes riesgos personales que podrían producirse tras identificar y analizar debidamente una alerta ocasionada en un edificio inteligente:

— Dirigir interactivamente a los ocupantes hacia ubicaciones seguras y a través de rutas de escape optimizadas, al objeto de evitar riesgos innecesarios que pudieran ponerlos en peligro.
— Inhabilitar los sistemas eléctricos, de ventilación o gas, que pudieran interferir o incrementar el riesgo identificado.
— Enviar información sobre la disposición y ubicación de elementos de utilidad (planos, extintores, etc.) al contingente afectado por la alerta.
— Alertar a autoridades o equipos de emergencia externos, dando cuenta de la situación en general respecto a la estructura, sus ocupantes y de los pormenores acontecidos.

Con este escueto ejemplo, se corroboran los enormes desafíos y las soluciones reales que nos depara el futuro tecnológico del IoT, que tendrán que ser abordados por empresas e industria integradas en consorcios empresariales, como es el caso de la Open Connectivity Foundation (OCF), donde miembros tan destacados como Cisco, Electrolux, Intel, Microsoft o Samsung Electronic intervienen en el desarrollo de estas nuevas tecnologías.

Ahora bien, el lector podrá preguntarse, ¿por qué se deja en manos de consorcios industriales el desarrollo de esta novedosa tecnología y no de instituciones públicas? Dicha cuestión es de fácil respuesta y cuanto menos curiosa, puesto que es el propio sector industrial el primer interesado en desarrollar y controlar todo el potencial del IoT, dependiendo de ello su éxito comercial y, por tanto, su supervivencia. Este potencial actuará como el valor real que sustentará la toma de decisiones de las corporaciones empresariales, acorde

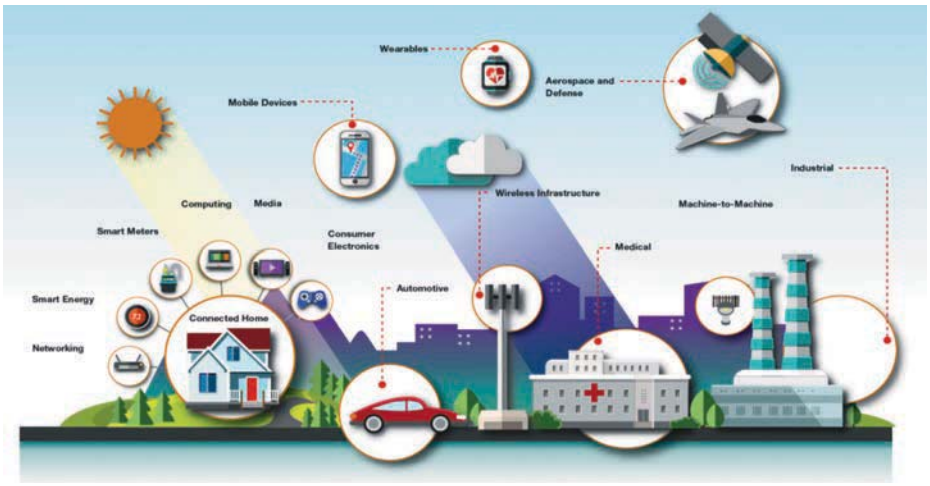


Diagrama dispositivos (IoT). (Fuente: *http://www.onemagazine.es/analisis-internet-de-las-cosas-alberto-hernandez-isms-forum-spain abril18*).

con la aceptación de esta tecnología por parte del mercado y de la calidad que sean capaces de aportar a los servicios disponibles en la red, relegándose finalmente a la «prehistoria» con esta ventaja competitiva las actuales técnicas de estudio de mercado, análisis de tendencias o la mera intuición.

Ahora bien, para que esta infraestructura sea eficiente, los diferentes dispositivos interconectados tendrán que actuar en base a un estándar, el cual delimitará sus procedimientos de interoperabilidad y, por supuesto, el marco de seguridad en el que operen. Estos surgirán igualmente de las corporaciones industriales, puesto que son ellas precisamente las que infieren conocimiento, fruto de la experiencia y de la feroz competencia industrial por la primacía en las nuevas tecnológicas.

Estándares, interoperabilidad y seguridad

Tal y como se ha mencionado, la principal faceta que caracterizará a los datos que operen en el IoT será su bajo ratio de emisión, puesto que constituirán conjuntos de datos reducidos y restringidos únicamente a atributos muy específicos o delimitados, tales como pudieran ser las lecturas características de un hogar inteligente (temperatura, humedad, etc.), la velocidad o el consumo instantáneo de un automóvil inteligente e incluso la frecuencia cardíaca de un marcapasos inteligente.

A pesar del gran volumen que lleguen a representar todas estas entidades, y precisamente por tratarse de datos reducidos a su mínima expresión, estos

podrán ser recopilados periódicamente sin convertir el proceso en un espectro de datos masivos (*big data*). Ello será posible, puesto que el IoT promulgará la recopilación y empleo periódico de datos generados por un sinfín de sensores y dispositivos, al objeto de verificar, determinar o condicionar en tiempo real el estado del sistema y, en caso de ser necesario, los propios dispositivos serán los encargados de desencadenar las oportunas acciones, al objeto de contrarrestar o neutralizar un estado o situación adversa para regresar al estado idóneo o programado.

Siguiendo con el ejemplo de vivienda inteligente, se llevará a cabo la captura periódica de datos generados por los distintos dispositivos de control y monitorización de la misma, los cuales serán analizados en tiempo real, y acorde a su estado podrían desencadenarse ciertas acciones correctoras para adaptar, por ejemplo, la temperatura de la vivienda, interoperando los sistemas de calefacción/refrigeración, o incluso empleándose la ventilación natural o forzada de acuerdo con los parámetros de estado interiores/exteriores de la vivienda. Una vez finalizada la cadena de procesos descrita, estos datos serán descartados y por tanto su validez será nula en la red, lo cual no impide que con independencia se decida su almacenamiento en una ubicación determinada.

A la hora de analizar importantes volúmenes de datos, existe un amplio espectro de herramientas predictivas, de tendencias o basadas en patrones de superficie, que permiten actualmente dotar a las corporaciones empresariales, del conocimiento suficiente para lograr cierta ventaja competitiva de cara a tomar decisiones futuras o interpretar situaciones pasadas. A pesar de lo cual este modelo de análisis contrastará con la filosofía de la IoT, puesto que el volumen de datos generado en un instante concreto mostrará directamente la imagen real y actualizada de un sistema, no dando lugar a predicciones, tendencias o análisis pasados.

En otro orden y extrapolando el volumen de datos tratados por la IoT, podremos considerar el espectro espacial que abarca la red como si de una macrovivienda inteligente se tratase. Dicho esto, sería posible establecer un marco que haga viable el desarrollo de sistemas inteligentes por parte de un gobierno para el tratamiento de datos generalistas, financieros, privados, etc. Estos sistemas, que interactuarían en tiempo real contra la red en base a un planteamiento de análisis concreto, harían factible, por ejemplo, la identificación de fraudes o actividades fuera de la ley.

A pesar de la claras ventajas que proporcionaría un procedimiento de estas características en pro de la Ley, claramente se trataría un sistema de vigilancia proactiva y, como consecuencia de ello, será primordial la investigación y el desarrollo de algoritmos que traten de identificar esta clase de situaciones o estados al objeto de perseguirlas. En sintonía con las características reseñadas para esta clase de infraestructuras, estas ventajas van asociadas igualmente a ciertos riesgos, sobre todo a la hora de tratar la temá-

tica de la seguridad individual y la gestión de la privacidad o el acceso a datos propietarios.

La protección y seguridad en las redes goza de plena actualidad y máxima relevancia; prueba de ello es que nos vemos continuamente sometidos al bombardeo de consignas y recomendaciones que tienen como objeto evitar accesos no autorizados o la protección de datos y a ubicaciones reservadas (corporativos y privados), tratando de impedir que nos convirtamos en víctimas de los innumerables riesgos a los que nos vemos expuestos al navegar por internet (fraude bancario, robo de identidades, etcétera).

Ahora bien, a la hora de observar las capacidades teóricas de la IoT, se identifican claramente nuevas formas de riesgo, que relegan los que ahora existen a la mera anécdota. Independientemente del gran impacto que pueda suponer una amenaza actual, esta dista años luz de los nuevos peligros y del impacto inherente que representa un acceso no autorizado a un «sistema inteligente». Actualmente una filtración de datos clasificados puede ser catalogado fácilmente como un hecho grave, muy grave o incluso catastrófico; pero prefiero dejar a criterio del lector la catalogación del efecto que puediera representar un acceso no autorizado al proceso de control de un vehículo inteligente, al hecho de inmiscuirse en un edificio gubernamental inteligente cuyos dispositivos sean capaces de captar imágenes y conversaciones o a tomar el control de una bomba de insulina instalada en un paciente.

Con la finalidad de garantizar únicamente los accesos previamente autorizados y un entorno de seguridad mínima que exigen los sistemas, equipos, dispositivos y sensores inteligentes, se hace imprescindible implementar métodos de encriptación y de interfaces independientes que garanticen por igual seguridad e interconectividad. Como consecuencia de ello, fabricantes, desarrolladores y proveedores de servicios tendrán que converger en un marco de seguridad estandarizado.

A pesar de disponerse actualmente del estándar *ZigBee* IEEE 802.15.4, el empleo de un sistema de encriptado basado en un cifrado avanzado de 128 *bits* (*Advanced Encryption Standard*, AES) debe complementarse con unas medidas adicionales de seguridad, al objeto de reducir el riesgo de accesos no autorizados a sistemas con un alto nivel de protección y superar así el grado de protección actual para un sistema crítico.

Futuras aplicaciones

Acorde con lo expuesto en este artículo, los entornos relacionados con el hogar inteligente y el mercado de productos electrónicos de consumo serán probablemente los de mayor interés y expansión empresarial. En la misma línea, la arquitectura del hogar inteligente abarcará un ámbito que solapará el actual concepto de casa conectada, en la que se integrarán diferentes dispositi-

vos inteligentes que interactuarán entre sí, además de disponer de la capacidad de conectarse al mundo exterior, lo cual repercutirá en un autoaprendizaje autónomo y un incremento de su nivel de prestaciones.

El primer paso implementado de cara al concepto de hogar inteligente fue formalizado con el diseño de dispositivos para la automatización de funciones básicas domésticas, es decir, la actual domótica. El interconexionado de estos dispositivos implementado mediante instalaciones de cableado, operadores de telecomunicaciones (*multi-system operators*, MSO), proveedores de servicios de Internet (ISP), etc., dispensan en la actualidad una extensa gama de dispositivos presentes en el hogar: moduladores, enrutadores, cámaras y sensores de seguridad, sistemas de control remoto, etcétera.

De igual modo que estos dispositivos ya no nos resultan novedosos, tampoco podemos catalogarlos de inteligentes a la hora de implementarse en una infraestructura de hogar inteligente, como consecuencia de las siguientes consideraciones:

— A pesar de que un equipo de domótica dispone de una electrónica independiente que le permite interconectarse con otros dispositivos domésticos, estos carecen de la capacidad suficiente de integración e interoperación entre ellos. Como ejemplo, hoy día no es posible procesar las señales de movimiento captadas por un dispositivo volumétrico para ser operadas por el sistema de calefacción o de refrigeración, y en este mismo sentido, un sistema de seguridad no dispone de la capacidad de activarse tras identificar un acceso no autorizado, puesto que no puede discernir entre el perfil del morador o del intruso.
— La inteligencia de un dispositivo será evaluada en función de su capacidad de procesado y de su autoaprendizaje a la hora de discernir cualquier variación del entorno, independientemente de su programación característica. Dicho esto, queda patente que todavía falta un largo trecho para que una cafetera sea capaz de preparar café al identificar que sus moradores se han despertado, o incluso calcular la cantidad de café necesaria en función de su tiempo de descanso.
— Cualquiera de los dispositivos mencionados dispondrán de un sistema de control propio, lo cual entra inicialmente en conflicto con la premisa de interoperabilidad que exige un sistema inteligente. Por ello, se perseguirá la estandarización de un programa de control universal de dispositivos, de igual modo que no disponemos de un mismo mando para el control de TV, DVD, equipo Hi-Fi, cafetera, lavadora, etcétera.

Dado que la idea de interoperabilidad entre diferentes sistemas, dispositivos, sensores y aplicaciones pueda parecernos algo más propio de un película futurista, nada más lejos de la realidad se nos presenta el servicio inteligente doméstico (*Smart Home as a Service*, SHaaS), el cual ya se encuentra disponi-

ble, siendo capaz de desarrollar una serie de funciones a modo de colección de servicios de mayordomo que serán operadas por los propios dispositivos una vez identificados ciertos estados del sistema y tras analizarse los datos aportados por los diferentes sensores del hogar. Por ello, la identificación de los diferentes estados del entorno será formulada como si de un proceso de aprendizaje se tratase, al objeto de convertir el hogar en un entorno lo más cómodo, seguro y energéticamente eficiente posible.

Actualmente para llevar a cabo la implementación de un SHaaS, es imprescindible disponer de los siguientes elementos básicos:

— Una red de sensores en el hogar, tales como cámaras de seguridad, sensores de movimiento, dispositivos de posicionamiento de individuos en determinados espacios, etc., capaces de generar los indispensables datos de entorno.
— Un servicio en la nube, donde se ubique la información generada por los sensores, sus datos de autentificación, así como el análisis del estado vigente. A esta ubicación se le asignará un nivel de seguridad suficiente como para poder proteger y disponer de los datos necesarios de un modo rápido y fiable.
— La administración remota de dispositivos mediante una interfaz que permita la parametrización e identificación del estado de entorno y a partir del cual se desencadenarán las acciones necesarias para la restauración del estado definido por el propietario.
— Un proveedor del servicio, como ente que proveerá el sistema (equipos e interfaces), además de gestionar y aportar la asistencia que monitoriza el entorno cliente.

Por supuesto, y tal como se ha citado, además de disponerse de una infraestructura que implemente los elementos enumerados, será imprescindible la habilitación de una conexión exterior, puesto que de nada sirve disponer de un sistema infalible si a la hora de identificarse una incidencia este no dispone de la capacidad suficiente para comunicarla a quien corresponda, en su entorno o en el exterior.

El segundo paso implementado para converger a una la infraestructura inteligente se sustentará en la interconexión de dispositivos mediante un método de comunicación fiable y viable, como es la actual internet. Esta tecnología permite implementar el ansiado control remoto de un sistema a través de una aplicación de escritorio o de un dispositivo celular, garantizando asimismo la interoperabilidad de sistemas y su autoaprendizaje.

Por descontado, esta demanda de interconexión para sistemas inteligentes exigirá la integración de protocolos *ZigBee* y *WiFi* dentro de un mismo entorno de sistema. Mientras el primero será el encargado de la gestión y comunicación entre dispositivos que actúan con un bajo ratio de energía, el WiFi

proporcionará servicio a los restantes dispositivos. Por tanto, en una infraestructura de estas características un sensor de movimiento *ZigBee* podrá interactuar con una cámara *WiFi* al objeto de transmitir, si cabe y a quien correspondiese, las imágenes de un probable intruso.

Actualmente, tanto investigadores como industria e incluso los propios MSO se encuentran inmersos en el desarrollo de soluciones integradas para el ámbito doméstico, la seguridad, el comercio o la gestión energética, dirigidos esencialmente a usuarios generalistas, clientes e incluso a sus propios empleados. A medida que estos sectores de negocio alcancen cotas de servicio cada vez más altas, ello se traducirá en un mayor aprovechamiento y expansión de todos los dispositivos inmersos en estas infraestructuras, como son los decodificadores, transceptores y receptores, que operado por un protocolo *ZigBee* lograrán alcanzar mayores cotas de SHaaS al objeto de lograr el ansiado concepto de hogar inteligente.

Más allá del entorno del hogar inteligente, la IoT presenta inicialmente unas posibilidades infinitas en el campo de la investigación, el desarrollo y la innovación (I + D + i) en campos tan dispares como la industria, la agricultura, el comercio, etc. A continuación se procede a realizar una pequeña introducción de las posibilidades que ofrece esta tecnología y el rumbo que llevan actualmente las investigaciones los diferentes sectores.

Agricultura

La implementación de la IoT en un sector como el primario puede cuanto menos sorprendernos, puesto que tendemos a asociar el I + D en su aspecto más tradicional. Nada más lejos de la realidad, la irrupción de esta nueva tecnología, con un empleo masivo de sensores, drones y procedimientos de análisis con los datos aportados por estos dispositivos augura un futuro muy fructífero para la agricultura, en el que se podrán abordar temas tan actuales como la optimización del rendimiento de los cultivos, la gestión de ganado, la explotación más efectiva de la tierra de labor, etcétera.

Como ejemplo, hará viable que la explotación de un agricultor pueda disponer de las siguientes capacidades:

— Gestionar sus recursos en modo remoto, en lugar de tener que comprobar *in situ* el estado de su siembra, del ganado, del riego, etcétera.
— Llevar a cabo la automatización de los procesos de la agricultura tradicional (siembra, recolección, etc.), lo cual repercutirá en la seguridad de los operarios.
— El proceso de automatización permitirá analizar, identificar y actuar en pro de la erradicación de plagas por parte de los propios elementos del sistema.

— Monitorizar y analizar los datos aportados por los diferentes dispositivos y sensores al objeto de identificar los patrones que permitan discernir el ciclo de crecimiento y alimentación para mejorar el rendimiento de una explotación.

Esta innovación irá dirigida en definitiva a conseguir el mayor rendimiento y la eficacia de una explotación agraria en función de sus correspondientes costes asociados y velando por la eficiencia energética derivada de los procesos agrícolas.

Transporte y logística

Los sectores del transporte y la logística constituyen uno de los campos en los que se están realizando mayores inversiones y estudios actualmente. El objetivo de este sector pasa por lograr el mayor ahorro de costes posibles, lo cual repercutirá necesariamente en el incremento de ingresos, valiéndose en todo momento de la posibilidad de deslocalizar centros logísticos y tratar de optimizar las rutas de transporte en función de los medios disponibles y las variables de entorno.

La irrupción de esta tecnología va de la mano de la automatización del parque móvil, constituyéndose un parque de vehículos inteligentes, y por tanto autónomos. Toda la información generada por los dispositivos de un vehículo autónomo intervendrán en un proceso de análisis que velará por la típica temática recurrente de los problemas logísticos, que se sustenta en la optimización previamente descrita.

Quién no ha imaginado un vehículo autónomo capaz de sacar provecho de toda la información disponible en tiempo real (meteorológica, el tráfico, consumos, destinos, etc.) y que el sistema realice la optimización del tiempo y coste de las rutas empleadas, repercutiendo en la seguridad de los usuarios y, por ende, en la reducción de la siniestralidad y de las primas de seguros.

Por supuesto, este conjunto de hitos no serán viables hasta que los diferentes sistemas inteligentes que se encargan de la monitorización del vehículo y de su entorno no sean una realidad. En este sentido, la actividad logística se verá potenciada por la monitorización de la mercancía mediante la integración de dispositivos de identificación y localización que, en combinación con el sistema inteligente, convertirán a un sector actualmente tan complejo en una actividad meramente rutinaria.

Un sistema inteligente con unas características como las mencionadas permitirá optimizar el consumo de combustible gracias a unas rutas idóneas, con restricciones de tráfico definidas y con unas condiciones meteorológicas determinadas, etc., todo ello analizado, procesado y operado en tiempo real.

De acuerdo con las capacidades de un sistema tan singular y a la hora de derivar un contenedor a un distribuidor determinado, se determinaría qué medio de transporte sería el más adecuado, así como la ruta a tomar acorde al tráfico, peajes, meteorología, etc., y todo ello en función no solamente de la optimización de costes y beneficios, sino que además se tendrían en cuenta otros restricciones, como la distribución de los centros logísticos, la disponibilidad de las dársenas de carga/descarga, la modalidad de servicio exigida por el cliente (urgente, ordinario, etc.), los patrones de oferta y demanda que automaticen y anticipen la dispensa de mercancía, además de su localización o ubicación exacta, y todo ello operado y gestionado en tiempo real.

Comercio minorista

La irrupción del IoT en el comercio minorista ofrece igualmente importantes oportunidades derivadas del importante ahorro de costes, que permitirá la automatización de procesos, la optimización de las operaciones y la mejora de nuestra imagen de cara al cliente.

Para ello resultará imprescindible el empleo masivo de dispositivos identificadores y localizadores de mercancías (*radio frequency identification*, RFID), lo que nos permitirá la automatización desde el proceso de inventariado hasta la ubicación de la mercancía en el canal de distribución o el consumo de un determinado artículo, todo ello en tiempo real. De este modo, podemos adelantarnos a una ruptura de *stock* y mecanizar el proceso de petición de mercadería o, por el contrario, exponer los excedentes a disposición de otros canales de distribución o formular ofertas directamente a la clientela.

Por todo ello, además de la agilización de los diferentes procesos, se logrará optimizar la dispensa de inventario, minimizar los tiempos del almacenaje o conocer el patrón de consumo de un artículo o en asociación con otros, temas esenciales cuando se trabaja en el sector de mercancías perecederas. Por supuesto, al gestionar este tipo tan singular de género, entra en juego otra gama de parametrizaciones fundamentales, como las características de una mercancía, clima al que deben permanecer en función del tiempo de almacenaje, su preferencia de salida en función de su estado, etcétera.

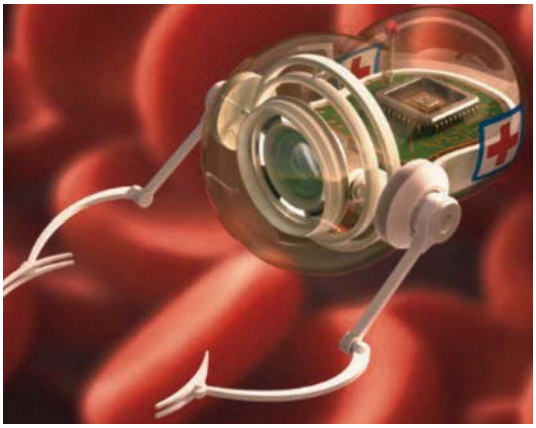
Toda la información disponible, fruto del análisis en tiempo real de los datos generados por los diferentes dispositivos inteligentes con los que cuenta el sistema, provocará el desencadenamiento de la operación en función del estado del entorno o del artículo en cuestión, por parte de los propios dispositivos. Como ejemplo, se actuará sobre el sistema de refrigeración ante un tiempo de almacenaje previamente definido para un artículo, el cual deberá verse interrumpido mediante su derivación al canal de distribución tras identificarse su deterioro que, en caso de no hacerlo, provocaría una desviación importante de los costes.

Por supuesto en este sector hay espacio para la mercadotecnia que, apoyada en un sistema de señalización digital, hace posible que un consumidor a través de un dispositivo móvil reciba las promociones vigentes en función de su perfil de consumo, conozca la ruta óptima a seguir para la adquisición de los artículos deseados, identifique su tallaje adecuado, sus preferencias o gustos, y todo ello sin ni siquiera encontrarse físicamente en el centro, desarrollando todo el proceso un carro autónomo en tiempo real.

Este campo tan innovador, no se restringe únicamente a la relación proveedor-cliente, sino que se propaga más allá, alcanzando campos como la optimización de inventarios, de sus canales de distribución e incluso el de la propia producción. Por tanto este sector puede identificarse como un eslabón intermedio, donde el cliente es el ente final de una larga cadena que podría transmitir al primer proceso que constituye la adquisición de las materias primas necesarias.

Medicina

Actualmente está de plena actualidad el empleo de sensores en el sector de la Medicina, los biosensores. Son dispositivos analíticos encargados de procesar un amplio espectro de parámetros biológicos, como puedan ser enzimas, virus, gases, iones y bacterias, generando una batería de datos sobre los que versará el correspondiente diagnóstico médico. Los dispositivos actuales son capaces de realizar un test de embarazo, análisis de glucosa en sangre de diabéticos, monitorización de los parámetros de células en sangre, análisis de fluidos corporales, identificación de trazas de ciertas proteínas, etcétera.



Nanotecnología médica. (Fuente: *https://www.cio.com/article/3043172/innovation/how-medical-robots-will-change-healthcarerhealth-get-familiar-with-it.html abril18*).

Dentro del campo de la Nanotecnología, se encuentra en plena efervescencia la ingeniería dirigida a la implementación de sistemas funcionales a nivel atómico, que a partir de un diagnóstico determinado operen en consonancia, tratando una dolencia o estado identificado. Su empleo e integración operacional no solo permitirá un rápido y preciso diagnóstico médico, sino que procederá de modo autónomo a aplicar prescripciones del medicamento a medida,

únicamente en la zona afectada, perfectamente localizada, y en función de las características individuales de cada paciente.

Una rama de la Nanotecnología se encuentra desarrollando nanorobots, dirigidos a combatir mediante diferentes técnicas, incluida la quirúrgica, dolencias muy definidas, como pueden ser un tumor delimitado, una obstrucción arterial, etc. Estos actuarían de modo autónomo sobre el problema identificado a través de un análisis previo tras la monitorización del paciente.

Este nuevo campo de la Medicina, que se asemeja más a la ciencia ficción, trataría de suplantar ciertas intervenciones quirúrgicas catalogadas como muy invasivas. Pero esto es ya otra historia… Innovación, investigación y desarrollo futuros.

ANEXO

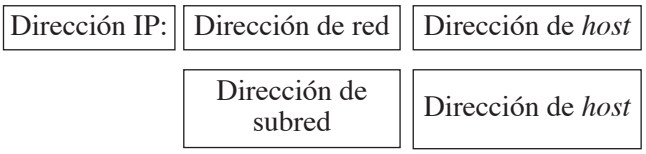
PROTOCOLO IPv4 *VS.* IPv6

El *Internet Protocol* (IP) forma parte del *Transmission Control Protocol* (TCP/IP) y es uno de los más importantes sobre los que trabaja internet, desarrollado originalmente por la Agencia de Proyectos de Investigación Avanzada (DARPA) del Departamento de Defensa de Estados Unidos.

Este protocolo trabaja bajo entrega de datagramas entre dos extremos de la red y sin conexión previa, siendo el responsable de seleccionar la trayectoria a seguir por cada uno de los datagramas, en función del tipo de servicio configurado. Asimismo será el encargado de llevar a cabo las pertinentes labores de fragmentación y reensamblado de datagramas.

Tal y como establece este protocolo, a toda computadora, nodo u otro dispositivo conectado que utilice los servicios de la red (*host*) le será asignada una dirección IP única. En sintonía con esta premisa y como consecuencia de la rápida expansión de la red y para lograr un diseño de estructura que englobase las distintas redes locales conectadas, fue necesario realizar la división lógica de la propia red en otras de menor tamaño. Este modelo de organización es el causante del término *subred*.

De acuerdo con la descripción, una subred posee existencia propia dentro de la red original, aunque no desde el punto de vista de la red exterior internet.



Para la representación de un *host* mediante una dirección IPv4, será necesario emplear un sistema de direccionamiento constituido por 32 *bits* de longi-

tud, que identificará por igual nodos y dispositivos de la red. De esta manera queda fijado el rango total de direcciones en aproximadamente 4.300 millones (4.300×10^6) direcciones únicas, que serán representadas mediante cuatro grupos de tres dígitos enteros cada uno y separados entre ellos por puntos.

Dirección IP: 123.101.102.003

De este modo, cualquier nodo o dispositivo requerirá de una dirección IP única para comunicarse a través de internet. El protocolo en su versión IPv4 fue adoptado por el Grupo de Trabajo de Ingeniería de Internet (IETF) en un momento incipiente del desarrollo y en el que parecía que este rango de direcciones articulado sería más que suficiente para hacer frente a cualquier demanda global de direcciones.

El protocolo IPv4 dispone de cinco tipos de formatos diferentes, que se dividen en:

— CLASE A: constituida por siete *bits* para direcciones de red ($2^7 = 128$ redes) y otros veinticuatro bits para el direccionamiento de *host* ($2^{24} =$ 16.777.216 *hosts*).

1	Dirección de red (7 *bits*)	Dirección de *host* (24 *bits*)

— CLASE B: constituida por catorce *bits* para direcciones de red y otros dieciséis *bits* para el direccionamiento de *host*.

1	0	Dirección de red (14 *bits*)	Dirección de *host* (16 *bits*)

— CLASE C: constituida por veintiún *bits* para direcciones de red y otros ocho *bits* para el direccionamiento de *host*.

1	1	0	Dirección de red (21 *bits*)	Dirección de *host* (8 *bits*)

— CLASE D: reservada para direccionamientos multidestino a un grupo específico de *host (multicasting)*.

1	1	1	0	Dirección *multicast* (28 *bits*)

— CLASE E: se trata de una clase con fines experimentales.

1	1	1	1	0	Reservada (27 *bits*)

Es importante recalcar que el siguiente rango y los dígitos asociados a los campos de dirección red o *host* se encuentran reservados, dado que su función se haya predefinida:

— 127.0.0.1 (*loopback*) se refiere a la propia máquina.
— O, se refiere a la red o al *host* local.
— 1, se refiere a todas las redes o *hosts*.

Por el contrario, este esquema de direccionamiento se presenta como una desventaja a la hora de cambiar un *host* de red, puesto que deberá hacerlo igualmente su dirección IP. Asimismo, si el tamaño de la red de destino varía en demasía, puede verse modificada la clase del formato de direcciones para adaptarse a las características de la subred.

Esta versión del protocolo IP se ve abocada a la fuerte limitación que imponen los campos de dirección en función de sus clases A, B, C y D, puesto que la expansión exponencial de equipos conectados en los últimos años exige la ampliación del espectro de direcciones, además de demandar una mayor seguridad, *calidad de servicio* (QoS) y efectividad en sus encaminamientos, lo cual ya provee la nueva versión IPv6, que presenta las siguientes mejoras respecto a la IPv4:

— Ampliación del espectro de direcciones, puesto que los campos de dirección pasan a disponer de una longitud de 128 *bits*.
— Mejora del mecanismo de opciones, que pasa a ubicarse en cabeceras separadas de la capa IP y de transporte. Dado que la mayoría de estas cabeceras no son examinadas por los dispositivos de encaminamiento, esto simplifica su enrutamiento.
— Direcciones de autoconfiguración, lo que la dota de capacidad de direccionamiento dinámico.
— Aumento de la flexibilidad de direccionamiento, incluyéndose la modalidad de monodistribución (*anycast*) a un nodo seleccionado.
— Facilidad de asignación de recursos, puesto que es posible etiquetar paquetes como pertenecientes a un tráfico especial, como pueden ser vídeo o voz.
— Seguridad que aporta al admitirse la autentificación y la privacidad.
— Eliminación de control de errores de cabecera.
— Fragmentación de paquetes únicamente en la fuente.

Esta nueva versión del protocolo fue definida formalmente en 1998 por el IETF, con objeto de reemplazar paulatinamente a la versión IPv4 y superar así

su gran limitación respecto al número de direcciones disponibles, implementando para ello un formato de direcciones de 128 *bits*, con lo que se alcanza del orden de 340 x 10^{36} direcciones únicas.

A la hora de tratar con el direccionamiento de IPv6, se destaca la asignación de direcciones que se realiza a interfaces individuales de los nodos y no a los propios nodos. De este modo, una única interfaz puede disponer de múltiples direcciones monodestino y estas podrán ser empleadas en la identificación unívoca del nodo correspondiente.

El primer campo que se incluye en una dirección IPv6 se refiere al prefijo de formateo, que es de longitud variable y que se emplea para la identificación de las tres categorías diferentes de direccionamiento que implementa:

— Unidistribución (*unicast*): un paquete con esta modalidad de direccionamiento es entregado a la interfaz identificada por esa dirección.
— Monodistribución (*anycast*): un paquete con esta modalidad de direccionamiento es entregado a una de las interfaces identificadas por esa dirección, la más cercana respecto a la definición realizada en su configuración.
— Multidistribución (*multicast*): un paquete enviado con esta modalidad de direccionamiento es entregado a todas las interfaces identificadas por esa dirección.

A modo de ejemplo se muestra a continuación, el formato de una dirección IPv6 en el que es posible identificar siete grupos, en los que se encuadra un número hexadecimal que representa dos octetos:

Dirección IP: 5566:678A:BF53:BBBB:FFFFF:EEFF:0000

BIBLIOGRAFÍA

ABI Research. (9 de mayo de 2013): *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020. ABI resarch for visionaries*, p. 1. *www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/*.

ASHTON, K. (22 de junio de 2009): «That Internet of Things». *RFID Journal*, p. 1. *www.rfid-journal.com/articles/view?4986*.

GARCÍA TOMÁS, J.; RAYA CABRERA, J. L., & RODRIGO RAYA, V. (2002): *Alta velocidad y calidad de servicio en redes IP* (vols. 503-9). Paracuellos del Jarama, Madrid, Ra-Ma.

MILLER, Lawrence (2017): «Internet of Things For Dummies». *Qorvo* Special Edition, vol. I. ISBN: 978-1-119-34992-1; vol. II. ISBN: 978-1-119-34989-1.

(openSAP) *https://www.sap.com/spain/trends/internet-of-things.html* abril 2018.