

Ángel Asensio Gimeno

Contribuciones a la
interoperabilidad y a la
optimización energética en el
diseño de dispositivos para la
Internet de las Cosas

Departamento
Ingeniería Electrónica y Comunicaciones

Director/es
Marco Marco, Álvaro
Casas Nebra, Roberto José

<http://zaguan.unizar.es/collection/Tesis>



Universidad
Zaragoza

1542

Tesis Doctoral

CONTRIBUCIONES A LA INTEROPERABILIDAD Y A LA OPTIMIZACIÓN ENERGÉTICA EN EL DISEÑO DE DISPOSITIVOS PARA LA INTERNET DE LAS COSAS

Autor

Ángel Asensio Gimeno

Director/es

Marco Marco, Álvaro
Casas Nebra, Roberto José

UNIVERSIDAD DE ZARAGOZA

Ingeniería Electrónica y Comunicaciones

2016



Departamento de
Ingeniería Electrónica
y Comunicaciones
Universidad Zaragoza



Universidad Zaragoza

Tesis Doctoral

Contribuciones a la interoperabilidad y a la optimización energética en el diseño de dispositivos para la Internet de las Cosas

ÁNGEL ASENSIO GIMENO

Directores:

Dr. Roberto Casas Nebra

Dr. Álvaro Marco Marco

Zaragoza, Noviembre 2015

Agradecimientos:

Resulta paradójico, que después de tantas páginas defendiendo la importancia de las Cosas en eso que llaman Internet de las Cosas, sin duda para mí, las siguientes líneas son las más importantes, puesto que no hablan de Cosas sino de Personas. Dicen que cualquier momento es bueno para dar las gracias, aunque posiblemente, no lo hagamos tan a menudo como debiéramos. Por ello, aprovechando que los convencionalismos dictan un apartado de agradecimientos, espero que se entienda que lo “haga un poco mío” y lo aproveche para dar las gracias...

Gracias a mis compañeros de HOWLab...

Que más que compañeros son amigos. Pues junto con Teresa, Rubén, Roberto, Álvaro (y Diego, ahora por Alemania), hemos pasado desde buenos ratos hasta Tormentas. Hemos compartido momentos de alegría y vivencias personales, pero es en los momentos duros donde sale la templanza de cada mujer y hombre. Ellos han demostrado ser esa clase de personas con las que, llegado el caso, uno puede lanzarse a cruzar hasta las mismísimas montañas del Tíbet. Hemos trabajado juntos y discutido, vaya que si hemos discutido!. Discusiones, algunas técnicas (CTP ha creado más polémicas que las interpretaciones de textos sagrados), y otras no técnicas. Muchas han durado días, e incluso se arrastran desde años, y no me extrañaría que algún día quizás se escriba una tesis sobre “Arco o Katana”. Pero en el fondo, es una gran suerte, pues de cada una de esas discusiones se sale un poquito más sabio de lo que se entró. Ojala todos pudieran tener semejantes compañeros.

Quiero agradecer especialmente el apoyo a Roberto y Álvaro, mis directores de tesis. Y aunque mi agradecimiento es grande, aun así no es ni la mitad que mi admiración por sus capacidades.

Carlos, no más, me alegra ver que el espíritu de HOWLab cruza océanos (y ojalá que en breves también lo hagamos nosotros).

...espero poder seguir no solo aprendiendo sino también avanzando con vosotros.

Gracias a aquellos con los que he tenido la suerte de crecer pero ya nos dejaron...

Sé que a ellos, esta tesis les habría hecho más ilusión de la que a mí mismo me hace. Lo hubiésemos celebrado unos con risas enconadas, otros henchidos de orgullo por su nieto ingeniero, algunos pensando alguna trastada mientras sonríen y se rascan la oreja, y otros dándome manotazos mientras me llamaban “pelgarucho”. Es ley de vida que ya no estén, pero también es necesario honrar su recuerdo en especial en los momentos importantes.

...vuestro recuerdo permanece y me guía cuando surgen las preguntas o el camino se endurece.

Gracias a las personas que me acompañan en mi día a día, a mi familia y amigos...

A mis amigos en especial a Belén, Joaquín, José Luis y Víctor, a los que conozco desde hace tanto que ya ni recuerdo.

A todos mis "tíos", con ellos he crecido, y de cada uno de ellos he aprendido algo. Interés por la ciencia, a preocuparse por los demás, a saber disfrutar el momento, a afrontar la vida con alegría sin importar los reveses.

A mi hermana Pilar. De la que no se puede estar más orgulloso y cuya alegría es contagiosa. Es la hermana pequeña, de la que el hermano mayor ha aprendido con orgullo numerosas veces. Alberto, cuñado, no me olvido de ti, y si he conseguido acabar una tesis, igual pueda subir al Moncayo contigo.

A mis padres, Ángel y Esperanza, sobre los que tanto podría decir, pero temo que si empiezo, mi tendencia a dispersarme haga desmerecer el mensaje. Solo diré, gracias, por estar siempre ahí pues buena parte de lo que soy es vuestro.

...creerme si os digo que estoy seguro, que no habrá carrera o tesis alguna que encierre el mismo conocimiento y sabiduría que el que vosotros me habéis dado.

Gracias a una persona recién llegada y que ha cambiado mi vida...

Dicen que una tesis es un gran momento, un hito importante para quien se ha embarcado en tamaña empresa. Para mí no es menos, pero sin embargo, cuando pase el tiempo, y recuerde estos días, seguro que sonreiré pensando en otra cosa.

...Isabel, espero contar siempre contigo.



**Departamento de
Ingeniería Electrónica
y Comunicaciones
Universidad Zaragoza**



Universidad Zaragoza

D. Roberto Casas Nebra, Profesor Titular Universitario del Departamento de Tecnología Electrónica y Comunicaciones de la Escuela de Ingeniería y Arquitectura de la Universidad de Zaragoza y D. Álvaro Marco Marco, Investigador del grupo HOWLab del Instituto de Investigación en Ingeniería de Aragón de la Universidad de Zaragoza.

CERTIFICAN:

Que la memoria de Tesis Doctoral “Contribuciones a la interoperabilidad y a la optimización energética en el diseño de dispositivos para la Internet de las Cosas” presentada por D. Ángel Asensio Gimeno, ha sido realizada bajo su dirección en el programa de Doctorado en Tecnologías Electrónicas (8-5008-1) y se corresponde con el Proyecto de Tesis aprobado por la Comisión de Doctorado. Por ello autorizan su presentación en la modalidad de compendio de publicaciones, cumpliendo con las condiciones requeridas para que su autor pueda optar al grado de Doctor por la Universidad de Zaragoza.

Y para que así conste, firman en Zaragoza a 9-Noviembre de 2015.

Fdo: D. Roberto Casas Nebra

Fdo: D. Álvaro Marco Marco

La presente Tesis Doctoral está constituida por un compendio de trabajos de investigación publicados y/o en proceso de publicación en diversas revistas de carácter internacional para optar al título de Doctor por la Universidad de Zaragoza, según el acuerdo del 20 de Diciembre de 2013 del Consejo de Gobierno, por el que se aprueba el Reglamento sobre Tesis Doctorales de la Universidad de Zaragoza.

A continuación, se presentan las referencias bibliográficas de cada uno de los artículos:

1. **“Hardware Architecture Design for WSN Runtime Extension”**. Ángel Asensio, Rubén Blasco, Álvaro Marco, Roberto Casas, International Journal of Distributed Sensor Networks, vol. 2013, Article ID 136745, 11 pages. doi:10.1155/2013/136745.
2. **“Energy-awareness application for the Internet of Things”**. Ángel Asensio, Rubén Blasco, Álvaro Marco, Roberto Casas, Teresa Blanco, Carlos Trasviña-Moreno, International Journal of Sensor Networks, ISSN: 1748-1287.(Enviado)
3. **“Protocol and Architecture to Bring Things into Internet of Things”**. Ángel Asensio, Álvaro Marco, Rubén Blasco, Roberto. Casas. International Journal of Distributed Sensor Networks, vol. 2014, Article ID 158252, 18 pages. doi:10.1155/2014/158252
4. **”Managing Emergency Situations in the Smart City: the Smart Signal”**. Ángel Asensio, Teresa Blanco, Rubén Blasco, Álvaro Marco, Roberto Casas. Sensors 2015, 15(6), 14370-14396. doi:10.3390/s150614370
5. **“Wireless Sensor Networks in Traffic Management Systems”**. Ángel Asensio, Carlos A. Trasviña-Moreno, Rubén Blasco, Álvaro Marco, Roberto Casas. Proceedings of the 6th International Conference on Applied Informatics and Computing Theory (AICT’15). Salerno, Italy.2015. ISBN: 978-1-61804-313-9

Los manuscritos 1, 3, 4 están publicados en revistas indexadas en el Journal of Citation Reports. El manuscrito 5 está publicado en el libro científico-técnico de Proceedings del 6th International Conference on Applied Informatics and Computing Theory (AICT’15). El manuscrito 2, ha sido enviado a la revista International Journal of Sensor Networks.

Adicionalmente, se debe mencionar, que los resultados de la presente tesis doctoral constituyen la base tecnológica sobre la que se han generado dos patentes, en las que el doctorando figura como coinventor. Ambas se encuentran en explotación por la empresa Implaser 99 S.L.L.:

“Intelligent system for signaling an emergency in tunnels” Núm. Solicitud: PCT/ES2014/070768 Núm. Fecha de prioridad: 14/10/2013. Fecha de publicación: 23/04/2015 País de prioridad: España. Empresas que la están explotando: IMPLASER 99 S.L.L

“Señal con retroiluminación inteligente y autónoma”.Núm. Solicitud: U201230980. Núm. Patente ES10777777. Fecha de prioridad: 25/09/2012. Fecha de concesión: 26/12/2012. País de prioridad: España. Empresas que la están explotando: IMPLASER 99 S.L.L.

RESUMEN

Actualmente estamos asistiendo al desarrollo de lo que se ha dado en llamar Internet de las Cosas o IoT (Internet of Things). El escenario futuro con el que se presenta IoT imagina que las Cosas que nos rodean son capaces de interactuar entre si y con nosotros mismos, en la mayoría de las ocasiones sin que seamos conscientes de ello, para de este modo ofrecernos algún tipo de servicio. Idealmente sobre estas Cosas no se necesitará ningún tipo de acción por nuestra parte, ni en la instalación, el mantenimiento o la configuración. Como si de un anuncio comercial se tratase cabría decir que “con IoT las Cosas que nos rodean se comunicarán y actuarán entre ellas de modo autónomo para hacernos la vida mejor y más fácil”.

El término de IoT es actualmente tendencia, y no son pocos los que vaticinan que cuenta con componentes para ser la próxima revolución tecnológica. Se considera que al igual que Internet revolucionó los paradigmas de interacción social, IoT puede suponer la revolución en la interacción con el entorno que nos rodea. No obstante hay posturas escépticas al respecto, unas se preguntan cuánto está tardando en llegar aquello sobre lo que se viene hablando durante estos últimos años y otras no consideran que llegará a ser la tecnología disruptiva que se promete.

Sea como fuere, y discusiones de este tipo aparte, está claro que actualmente IoT es un movimiento tecnológico que despierta interés y expectación, de hecho se considera que IoT es una tendencia dentro de las previsiones tecnológicas. No obstante como cualquier tecnología que está en su fase inicial, no es suficiente con ilusionar, sino que para conseguir su desarrollo y penetración en la sociedad, el interés por ella tiene que venir acompañado por una utilidad real. IoT crecerá solo si su uso supone un beneficio, lo que en última instancia suele cuantificarse en términos económicos.

Los analistas consideran que el beneficio económico en IoT provendrá de la manipulación de la información y la generación de servicios. Quizás por ello, las descripciones generalistas de IoT, su exposición mediática, sus estimaciones y análisis de negocio, etc. parecen venir dados desde la óptica de aquellos más relacionados con el ámbito de la información, de Internet. De igual modo, quizás porque el propio nombre de IoT así parece animarlo, la mayoría de desarrolladores de esta nueva concepción tecnológica provienen de áreas próximas a Internet. Esto parece validado por la percepción que pudiera tenerse de que, la creación de servicios a través de Internet, puede ser un mercado altamente rentable.

No obstante, un enfoque muy centrado en Internet, puede pasar por alto la otra parte del binomio IoT, las Cosas. No hay que olvidar que es necesario interconectar todas las Cosas a través de Internet, algo que no es sencillo y para lo que no existe consenso de como se ha de llevar a cabo. Como se desarrollará posteriormente, es como si “cada Cosa hablara su idioma y todas ellas tuvieran unas necesidades para poder funcionar”.

De lo que no hay duda es que para que IoT se materialice, todas las Cosas deberán incorporar una parte tecnológica, y más en concreto “una electrónica”. Una electrónica que, como algo tangible que es, tendrá sus limitaciones. Y es aquí precisamente donde surge la motivación de esta tesis, reflexionar sobre la situación actual de IoT, con un enfoque centrado en las Cosas. En el proceso se han encontrado algunas barreras y se ha pretendido realizar aportaciones que contribuyan a su superación.

Como punto de partida se realizó una revisión del estado del arte. El concepto IoT es algo abstracto y complejo, y puede abordarse desde diferentes perspectivas. Por ello se consideraron el conjunto de tecnologías implicadas en IoT y los servicios que puede llegar a ofrecer.

Basándose en los estándares y normas existentes, y a partir de una aproximación semántica al concepto de contexto y Cosa, se ha propuesto una especificación de protocolo, al que se ha denominado Common Things Protocol (CTP), desarrollado para facilitar la interoperabilidad entre las Cosas. El objetivo, es facilitar la compatibilidad con diferentes estándares de comunicación y permitir una implementación de modo sencillo y eficaz, en consonancia con los recursos limitados de las Cosas. Adicionalmente, la solución propuesta debe ser capaz de integrarse en la mayoría de las soluciones de IoT barajadas actualmente, por lo que para facilitar esto, se propondrá una arquitectura basada en el uso de un Gateway a modo de concentrador de protocolos y puente de interconexión con la red.

Otro de los requisitos necesarios de las Cosas de IoT es la ubicuidad. Esto tiene una doble implicación tanto temporal como espacial, y ambas impactan principalmente con las características tecnológicas en materia de comunicaciones y gestión de la energía. La demanda de energía en cualquier lugar y en cualquier momento obliga a las Cosas a usar eficientemente la energía disponible. A la hora de abordar el diseño del dispositivo se deberán tomar una serie de decisiones sobre los componentes, la arquitectura electrónica y los ciclos de operación del dispositivo. Para poder cuantificar la idoneidad de esas decisiones se requerirán tanto un correcto modelo energético del dispositivo como mecanismos para caracterizar en la práctica el consumo. El objetivo de la tesis es ofrecer herramientas en los campos anteriores, y ofrecer criterios que faciliten el diseño teniendo en cuenta la eficiencia energética.

Durante el desarrollo de la tesis, se tomó conciencia de la necesidad de disponer de estrategias para evaluar las diferentes propuestas, por lo que se abordó el campo de los factores de calidad de servicio (QoS) y las métricas de operación. Estos parámetros no solo resultarán útiles para cuantificar el comportamiento, sino que, si el propio sistema es capaz de ser consciente de su evolución, dispondrá de un mecanismo para ser capaz de autodiagnosticarse. Este aspecto es algo sobre lo que se tiene intención de seguir trabajando.

Por último, y quizás desde el punto de vista ingenieril, uno de los aspectos más apasionante y gratificante, se ha abordado la concreción de las ideas anteriores en algo real. En el marco de la tesis, y gracias a la participación en diferentes proyectos de investigación, se han podido desarrollar sistemas reales, que operan siguiendo la arquitectura IoT, en los que plasmar los conceptos anteriores. Como dijo Theodore Von Karman “Los científicos estudian el mundo tal como es; los ingenieros crean el mundo que nunca ha sido”, siendo IoT uno de los mecanismos más prometedores de crear ese futuro mundo. El mero hecho de haber visto sus comienzos e incluso participar en ello, es objeto de orgullo para cualquier Ingeniero.

Keywords: Internet de las Cosas, IoT, Interoperabilidad, diseño electrónico de bajo consumo, WSN.

CONTENIDO

1	Introducción.....	15
1.1	Internet de las Cosas.....	15
1.1.1	Historia y evolución de IoT.....	19
1.1.2	Arquitectura de IoT.....	24
1.1.3	Las Cosas en IoT.....	26
1.1.4	Métricas en IoT.....	39
1.1.5	Retos de IoT.....	42
1.2	Descripción del trabajo de tesis.....	45
1.2.1	Organización de la tesis.....	45
1.2.2	Motivación de la tesis.....	47
1.2.3	Objetivos de la tesis.....	50
1.2.4	Metodología de la tesis.....	53
2	Publicaciones.....	55
2.1	Hardware Desing for WSN Runtime Extension.....	57
2.2	Energy-Awareness Application for the Internet of Things.....	71
2.3	Protocol and Architecture to Bring Things into Internet of Things.....	85
2.4	Managing Emergency Situations in the Smart City: The Smart Signal.....	105
2.5	Wireless Sensor Networks in Traffic Management Systems.....	135
3	Conclusiones y trabajo futuro.....	147
3.1	Conclusiones.....	147
3.1.1	Contextualización de IoT: Situación actual y expectativas.....	147
3.1.2	Aportaciones al bajo consumo.....	148
3.1.3	Aportaciones a la interoperabilidad.....	149
3.1.4	Aportaciones a los mecanismos de evaluación de IoT.....	150
3.1.5	Implementación práctica e integración de sistemas de IoT.....	151
3.2	Trabajo futuro.....	153
4	Apendices.....	155
4.1	Apéndice 1: Características de las publicaciones.....	155
4.2	Apéndice 2: Contribución del Doctorando y renuncia de los coautores no doctores.....	157
4.3	Apéndice 3: Participación en otros resultados.....	159
4.4	Apéndice 4: Vision economica y social de IoT.....	161
4.4.1	Contexto.....	161
4.4.2	Situacion de mercado de la IoT.....	164
4.4.3	Impacto Social de la IoT.....	173
5	Bibliografía.....	179

1 INTRODUCCIÓN

1.1 INTERNET DE LAS COSAS

Internet se presenta en numerosas ocasiones como una gran disrupción y tecnología habilitadora (Latzer 2009) que además ha generado un gran impacto en las interacciones, actividades y organizaciones sociales (Bargh, McKenna 2004). Para algunos (Trappeniers et al. 2013), la siguiente revolución tecnológica se encontrará en el mismo ámbito: lo que se ha dado en llamar Internet de las Cosas o IoT (Internet of Things). Si Internet cambió la relación entre las personas, ahora se espera cambiar la relación de las personas con los objetos que las rodean.

El paradigma de IoT propone que todos los objetos que nos rodean a diario estén interconectados a través de Internet, siendo sus características y usos globalmente accesibles entre sí de modo ubicuo, es decir, en cualquier lugar y momento. Esto implica su integración en un nuevo contexto que permitirá la interacción entre las Cosas, con la finalidad de liberar a las personas de la necesidad de actuar sobre ellas y ofrecer nuevos servicios generados a raíz de la cooperación entre las propias Cosas. Uno de los requisitos implícitos de IoT es que las Cosas tienen que ser accesibles y operables de algún modo, total o parcialmente vía Internet. Esta capacidad de acceso a través Internet y el enfoque principal de la interacción entre las Cosas (y no solo entre las Cosas con las personas) marca la diferencia frente a otras propuestas tecnológicas previas como las redes de control industrial, las WSN (Wireless Sensor and Actuator Network) o los entornos inteligentes.

El concepto de Cosa debe ser considerado en el sentido más amplio de la palabra, como una entidad, ya sea real o virtual, que tiene relevancia en un determinado contexto y tiempo, y posee una identificación unívoca (Asensio et al. 2014). El término Internet, referido a estas Cosas, pretende transmitir la idea de que las mismas están intensamente comunicadas e interrelacionadas entre sí y con Internet. De modo simplificado, podríamos decir que IoT se basa en evolucionar las Cosas (Things) a Cosas Inteligentes (Smart Things) considerándolas entidades ubicuas, dotadas de cierto nivel de inteligencia y conectividad, capaces de interoperar entre sí y a través de Internet. Sin embargo, en contraposición al mundo de Internet, donde los recursos presentan una componente abstracta y formal muy elevada, las Cosas son elementos reales, dependientes de aspectos como la energía, memoria, potencia de cómputo, comunicaciones, etc., que generalmente son limitados.

Por ello, para el desarrollo de IoT, no basta con conectar Cosas a Internet, sino que estas tienen que ser interoperables entre sí, intercambiando información e interactuando con el entorno y las personas de un modo mínimamente intrusivo. Los objetos, y la computación tras ellos, han de pasar desapercibidos, es decir, tienen que ser autónomos, y superar sus limitaciones físicas, principalmente su dependencia energética.

Más allá de las consideraciones técnicas, se tiene que asumir que IoT se desarrollará solo en tanto en cuanto los servicios que ofrezca sean de utilidad a la sociedad, lo que al final inevitablemente implica un componente de beneficio de mercado, algo que es previsible que ocurra en breves. Así, según un informe del McKinsey Global Institute (Manyika et al. 2013), IoT está considerada como la tercera tecnología más disruptiva para la próxima década, con un volumen de negocio estimado de entre 2,7 y 6,2 billones (europeos) de dólares. Junto a ella, ocupan lo alto de la clasificación otras tecnologías como: Internet móvil (de 3,7 a 10,8 billones), automatización del conocimiento (de 5,2 a 6,7 billones) y tecnologías en la nube (de 1,7 a 6,2 billones) todas ellas estrechamente relacionadas entre sí y con IoT. En su informe “The Digital World in 2030” (Linton, Jaokar 2014), el EIF (European Internet Forum) remarca la importancia que puede tener IoT para las personas, y como la Unión Europea debe adoptar una posición de referencia al respecto, y convertirse en un actor principal.

ESCENARIO TÍPICO.

Una forma sencilla de exponer el concepto de IoT es mediante la descripción de un posible escenario, en el que se muestre su capacidad para prestar una serie de servicios de modo ubicuo y universal con una tecnología que pase desapercibida. A continuación, se ha tomado la libertad de “novelar un futuro próximo, con un estilo alejado del tecnicismo”. El objetivo es resaltar las repercusiones de IoT en las personas y la sociedad y exponer sus capacidades, algunas de las cuales ya son posibles actualmente:

“Jueves 22 de octubre, 07:40 horas. Suena el despertador. Normalmente te despierta algunos minutos más tarde, pero ha revisado tu agenda y hoy tienes una importante reunión. Tu cama le ha informado que ayer traspasaste y además, por tus excesivos movimientos, parece que no has pasado buena noche. El despertador ha estado monitorizando tu ciclo de sueño, así que ha seleccionado el mejor momento para despertarte, apurando la hora al máximo posible. Se encienden gradualmente las luces y la radio. Aunque normalmente tu asistente digital en el hogar sabe que no te gusta que interfiera, hoy ha decidido que agradecerás la ayuda. Prepara el baño y activa la ducha, te avisa que esta lista, y pone las noticias ya clasificadas en el monitor del baño para llamar tu atención. La temperatura y presión del agua se van adaptando para conseguir despejarte, el ciclo de hoy es más vigoroso y rápido. Tan pronto acabas, el asistente proyecta en el armario tu avatar con la vestimenta recomendada, acorde a tu agenda, climatología y a la ropa disponible. Aprovecha para recordarte que varios de tus trajes están en el tinte. Suelen recogerlos en persona, pero en esta ocasión pides que te los envíen. Tras vestirte, caes en la cuenta de que tienes que revisar la configuración de estilo, últimamente las propuestas son algo distintas. No es la primera vez que te arrepientes de haber dado acceso a tu perfil de preferencias de hábitos diarios, pero sonríes al ver la otra mitad del armario y recordar que tú también tienes privilegios de acceso; un día de estos alguien va a

acabar con algo más llamativo que de costumbre. La advertencia de que el café ya está listo, te saca de tus pensamientos.

Desayunas fuerte, bastante más que de normal, el frigorífico informa de ello a tu dispositivo personal de actividad física. Por lo visto la báscula del baño también se ha debido chivar de los excesos de este fin de semana; hoy no te apetece aguantar los destellos rojos de tu brazalete con cada galleta extra que comes, así que decides desactivarlo. Tienes el frigorífico bajo mínimos, por lo que te pide confirmación para programar el próximo pedido. Estás pendiente de recibir un par de libros y otras cosas, quizás salga rentable que la misma empresa de logística y venta online que te los envía, gestione tu compra de alimentos, y pase a por los trajes. Informas que no tienes urgencia en ningún envío, aunque quizás tu armario no piense igual. De cualquier modo, que se pongan de acuerdo entre ellos.

Se enciende el recibidor y la cocina se va oscureciendo. El tiempo se ha echado encima y te están animando a marchar. Al pasar por el recibidor, el mango del paraguas emite unos ligeros destellos en verde. Perfecto, hoy pronostican buen día. Al salir de casa, el reloj vibra insistentemente, te has dejado algo: Te recuerda si llevas el portátil, y efectivamente, tienes que volver a por él. Ahora sí, sales de casa, confiando en que el sistema de gestión se encargue de apagar las luces, cerrar las persianas y demás. El ascensor ya te está esperando. Lo habrá llamado la puerta de casa, o quizás tu smartphone, o el reloj, o las llaves del coche... Hubo un tiempo en que era necesario configurar estas vinculaciones, pero con la mejora de la inteligencia artificial distribuida, que aprende de tus hábitos, ahora es automático. Entrás en el ascensor, y este asume que vas al garaje. Menos mal porque no tenías las manos libres.

Al entrar en el coche, el asistente digital del mismo consulta la agenda de tu teléfono para verificar el destino. El navegador recolecta información de los servicios de tráfico, tus historiales previos de ruta e incluso contacta con los coches de compañeros en ruta para recabar información de primera mano y calcular el recorrido óptimo. Durante el trayecto, el asistente te informa que posiblemente llegues tarde a la oficina. Le pides que avise, así que manda un email excusando tu tardanza, e inicia una llamada a un compañero. Vuelven a sorprenderte los mismos baches que el viernes pasado. El asistente ya los detectó, analizó e informó de ellos al sistema de gestión de tráfico de la ciudad. De hecho, te acaban de responder que la incidencia se solucionará en unos días, y agradecen tu colaboración enviando al asistente del coche unos minutos gratis para los parquímetros del centro. Siempre has pensado que la colaboración digital ciudadana es importante, no te cuesta mucho que algunos de tus sistemas compartan la información como en este caso, las incidencias en ruta. Eso sí, aprovechas las circunstancias para verificar que el perfil de compartición de datos solo está activo para servicios de confianza; la colaboración es útil, pero también es necesario saber preservar la

intimidación digital. No te apetece oír la oferta del día cada vez que pasas por las proximidades de un comercio, ni aunque gracias a ello te propongan descuentos. Cuando estas llegando, el parquin envía su estado a tu asistente, y ambos intercambian horarios para buscar la plaza más cercana al ascensor que tienes que utilizar. Se solicita una pre-reserva de plaza; hoy has tenido suerte y el sistema te asigna una plaza al lado de la salida.

Ya en el trabajo, algunos de tus wearables avisan a tu asistente digital en la oficina que tu ritmo está disminuyendo, de modo que a través de un mensaje emergente en tu ordenador, te recomienda un almuerzo. Te propone algo ligero; por lo visto ya son oficiales los excesos del fin de semana y el desayuno, seguro que la cinta de correr del gimnasio también está al tanto y ya ha programado 15 minutos más para esta tarde. No te gusta almorzar solo, así que informas al asistente en la oficina que no te importa esperar hasta media hora más para almorzar y que se encargue de concretar una hora para coincidir con algún compañero. Decides confiar en su criterio, y dejas que lance la petición a la cafetería. Suele acertar, y así te evitas esperas.

Acudes a tu reunión con el ingeniero de inclusión en IoT de la empresa que os suministra el mobiliario de oficina. Pertenece al departamento de programación del asistente digital del edificio y últimamente has estado trabajando en la monitorización de hábitos de usuarios para mejorar la calidad del entorno de trabajo. Se ha conseguido una mayor productividad y confort, paradójicamente, disminuyendo las horas laborales y con un ahorro energético. El ingeniero de inclusión en IoT, os propone sustituir parte del mobiliario de vuestras oficinas por la nueva gama que incorpora sensores biométricos (para el usuario) y mecánicos (para el mueble). Pretende hacer un estudio de interacción con el usuario, evolución postural a lo largo del día para mejorar el confort y otros aspectos. Suena interesante. Le comentas que en caso de aceptar, por descontado exigirás el no almacenamiento de información local y un anonimato total. Pides conectividad de salida de su subred IoT únicamente a través de tus proxys, te comprometes a no usar, ni almacenar sus datos, pero quieres verlos... "tus fuentes de datos, tus normas". Prefieres ser cauto, recuerdas haber oído un incidente antes de tu incorporación. La empresa que gestionaba los equipos de vending "olvidó comentar" que también monitorizaba parámetros ambientales en torno a sus máquinas, en teoría para mejorar la eficiencia de las mismas. La información extraída no era crítica, pero no gustó que terceras personas pudieran inferir el estado de actividad en el edificio en tiempo real.

Volviendo al presente, no solo está de acuerdo con tus normas, sino que te permitirá la utilización de los datos, e incluso te facilitará los resultados ya procesados. Claro que te pide una renuncia a un uso comercial, algo totalmente lógico. Le comentas que esa información te será útil, y que podríais tratar de correlar sus datos con otras métricas de confort y eficiencia

que ya posees. Ni que decir tiene que se muestra muy interesado. Parece que va a ser una operación muy interesante y provechosa para ambas partes...“

Tal y como se aprecia en el escenario propuesto, los ámbitos de aplicación de IoT son diversos y muy heterogéneos. Como ha ocurrido con otras tecnologías, las aplicaciones de IoT serán cada vez mayores y ofrecerán servicios que a fecha de hoy ni se han considerado. Con todo, actualmente los entornos de mayor presencia de IoT son:

- Gestión de hogares, edificios y vecindarios (Xu Li et al. 2011) en sus diversos aspectos, como seguridad, monitorización ambiental y energética (Kelly, Suryadevara & Mukhopadhyay 2013), etc.
- Junto al ámbito del hogar, la ciudad constituye uno de los escenarios típicos de aplicación de IoT. El concepto de Ciudad Inteligente (Smart City) se encuentra estrechamente unido a la idea de IoT (Perera et al. 2014b), (Vlacheas et al. 2013).
- Aplicaciones en grandes espacios, como en la monitorización medioambiental (Lazarescu 2013), agricultura (Kaloxylou et al. 2012) o la gestión de emergencias (Yang, Yang & Plotnick 2013).
- En entornos industriales, empresas y sistemas de producción (Bi, Da Xu & Wang 2014), (Da Xu, He & Li 2014).
- Servicios relacionados con el ámbito social o personal, como redes sociales digitales (Atzori et al. 2012), apoyo a personas con discapacidad (Domingo 2012) o el sector de la salud (Fan et al. 2014).

1.1.1 HISTORIA Y EVOLUCIÓN DE IOT

La idea de interconectar los dispositivos y sistemas viene de lejos, visionarios como Nikola Tesla ya supieron intuirlo en fechas tan tempranas como 1926 (Kennedy 1926), aunque los primeros logros reales se consiguen en los 70s. En 1969 se crea el primer enlace entre las universidades de UCLA y Standford por medio de la red telefónica conmutada, en 1972 se realiza la demostración pública de ARPANET con protocolo NCP, sustituido por el actual TCP/IP en 1983. En 1990 se implementa el primer servidor Web basado en HTML en el CERN (M. Leiner et al. 2009). Con la introducción del concepto de computación ubicua por parte de Weiser en 1991 (Weiser 1991), se siembra el germen de la idea, de que todos los elementos que nos rodean pueden ser capaces de computar de manera transparente para las personas de su entorno. En paralelo, en el ámbito industrial en los años 80 empiezan a surgir las soluciones SCADA (*Supervisory Control And Data Acquisition*), en forma de sencillas redes de sensores y actuadores que interactuaban con el entorno para controlar un proceso productivo. Estos, pueden considerarse los primeros casos prácticos de lo que se entenderá por IoT en ambientes industriales.

Los posteriores avances en las comunicaciones inalámbricas, microelectrónica, sistemas embebidos y baterías hicieron posible distribuir pequeños dispositivos con diferentes niveles de inteligencia en los entornos. Gracias a esto, surgieron los llamados entornos inteligentes a los que por extensión se suele hacer referencia con el término AmI (Ambient Intelligence), por ser el soporte sobre los que se desarrolla esta inteligencia ambiental. Esta tecnología pretende facilitar la interacción de las personas con su entorno, para que sea llevada a cabo de modo natural, intuitivo y desentendido (*pervasive computing*), en todo momento y lugar (*ubiquitous*) y de tal modo que la tecnología sea consciente de la propia situación de su entorno (*context awareness*) (Remagnino, Foresti 2005). Los entornos inteligentes no son una tecnología en si misma sino una solución basada en un sistema complejo que requiere del uso de un número elevado de disciplinas tecnológicas, al igual que la actual IoT (Cook, Augusto & Jakkula 2009). Una de las líneas de investigación básica que ha estado más relacionada con ellos han sido las WSN ya que constituyen el esqueleto básico de comunicación e intercambio de información de todo entorno inteligente. Las WSN actuaron como tecnología base para implementar AmI (Kulkarni, Förster & Venayagamoorthy 2011) y con ello se avanzó hacia la visión propuesta por Weiser. Inicialmente, al hablar de entornos inteligentes o AmI, estos tenían sus límites bien definidos (hogar, oficinas, etc.), pero con la evolución de Internet como red global comienza a tomar fuerza el concepto de un solo espacio que permita a todos los elementos interconectarse entre sí. Puesto que se había dicho que Internet permitió conectar a todas las personas, se viene a proponer que esta misma Internet permitiese conectar también a todas las Cosas (Cook, Das 2012). Con ello hoy en día, se considera que el concepto de entorno inteligente está ligado a IoT, asumiendo que uno de los mecanismos más eficientes para generarlo es mediante la aplicación de IoT en ese entorno. Bajo esta premisa se puede considerar que IoT incluye o hace uso de conceptos previos como WSN, AmI, etc. (Perera et al. 2014a). Por su parte, en el ámbito industrial, las antiguas redes de automatización, han evolucionado de redes SCADA locales, a PLCs (*Programmable Logic Controllers*) y RTUs (*Remote Terminal Units*). Durante esta evolución, las WSN también jugaron un importante aspecto en el ámbito industrial, pudiendo incluso afirmarse que gran parte de los avances de las mismas fue justamente debido a su uso intensivo por parte de la industria (Gungor, Hancke 2009). Finalmente se abandonó el ámbito local para permitirse la telegestión a través de Internet (Galloway, Hancke 2013). Hoy en día se habla de varias fases en la evolución de los controladores industriales: monolítico, distribuidos, en red (National Communications Systems 2004), y actualmente como parte de IoT (Zuehlke 2010).

La primera constancia publicada que se tiene del termino IoT es del 2009 realizada por Keven Ashton (Ashton 2009), en el marco del uso de la tecnología RFID como mecanismo de optimización de la cadena de suministro en Procter&Gamble, aunque en 1999 el concepto de un dispositivo o Cosa conectado, utilizando la recién creada Internet ya fue comentado por Neil

Gershenfeld (Gershenfeld 1999). En 2005, comienza a encontrarse el término IoT entre alguno de los títulos de los libros de la UIT (Unión Internacional de Telecomunicaciones). En el 2009 el término ya aparece en varios artículos (Mattern, Floerkemeier 2010), estando muy ligado inicialmente al concepto de RFID (Welbourne et al. 2009), pero rápidamente se tomó conciencia de que IoT era algo más amplio e iba a ser la gran evolución de Internet (Atzori, Iera & Morabito 2010). En 2011, la empresa de asesoría Garner Inc. empieza a considerarla como una tecnología emergente. En 2012 IoT centró la conferencia sobre Internet más importante de Europa (LeWeb). Las revistas más populares de corte técnico generalista (Forbes, Fast Company, Wired, etc.) empezaron a hacerse eco del fenómeno IoT. En Octubre de 2013, la consultora IDC publica un informe poniendo de manifiesto el gran volumen de mercado previsto para IoT en un futuro próximo (Lund et al. 2013). En el “Consumer Electronics Show” (CES) de las Vegas de 2014, IoT tuvo una presencia muy preeminente.

En los últimos años, las iniciativas y proyectos relacionados con IoT se han visto incrementados en número y objetivos a lo largo de todo el mundo (Whitmore, Agarwal & Da Xu 2014), (Stankovic 2014). Como el concepto de IoT está comenzando a ser tremendamente popular ya han aparecido sistemas que aseguran ofrecer soluciones IoT al usuario final sin requerirle grandes conocimientos técnicos (Swan 2012). Con todo, los desarrollos actuales están en las primeras fases y la mayor parte de los servicios están basados en la monitorización o sensado de variables para extraer información del contexto, analizarla y mostrarla (López et al. 2012).

ESTANDARIZACIÓN EN IOT

Ha habido un elevado número de intentos de establecer diferentes niveles de estandarización para los protocolos de IoT. Los primeros de ellos, surgieron a modo de propuestas de organismos de investigación o entidades individuales (Palattella et al. 2013). Conforme IoT ha ido alcanzando mayor relevancia, se ha asumido que la estandarización vendrá dirigida desde consorcios tecnológicos, agrupaciones de empresas u organismos reguladores. Algunas de las pasadas propuestas han conseguido una mayor repercusión, en general debido a que detrás de la especificación se encontraban empresas de calado en el ámbito de las TIC. Así por ejemplo a finales del 2013, surgió una escalada mediática de noticias que presentaban el protocolo MQTT (*MQ Telemetry Transport*) (MQTT 2015) promovido por IBM como un futuro standard para IoT, aunque finalmente, esta propuesta se estancó. A continuación se repasan las iniciativas actuales más importantes.

AllSeen Alliance (AllSeen 2015), presentada en el 2013 es un consorcio sin ánimo de lucro, liderado por Qualcomm, que cuenta con la participación de más de 50 empresas, entre sus miembros premier se encuentran Microsoft, Cisco y la Linux Foundation. Su objetivo es la difusión de productos, sistemas y servicios que soporten IoT con un *framework* universal y abierto basado en AllJoyn. AllJoyn es un proyecto Open Source, presentado en el “Mobile World

Congress” del 2011 por Qualcomm, que provee un *framework* y un conjunto de servicios para permitir la interoperabilidad entre dispositivos y aplicaciones a través de la creación de redes próximas dinámicas utilizando una comunicación D-Bus; actualmente la capa de comunicación (y con ello el hardware) está limitado a Wi-Fi.

De modo similar se presentó en el 2014 Open Interconnect Consortium (OIC) (OIC 2015) un grupo liderado por Intel y Dell, que incluye a empresas como Atmel, Broadcom (fundadora, pero que abandonó posteriormente el consorcio), Dell, Samsung y Wind River. Se centra principalmente en la creación de un estándar abierto para la interconexión *wireless* entre dispositivos y su interoperabilidad a través de Internet, proponiendo el uso de CoAP (Bormann, Castellani & Shelby 2012) en la capa de aplicación.

También en 2014 se fundó el Industrial Internet Consortium (IIC) (IIC 2015) que agrupa a más de 130 miembros (siendo fundadores AT&T, Cisco, General Electric, IBM, e Intel) con el objetivo principal de desarrollar estándares para el uso de IoT en la industria. Hasta la fecha sus acciones se han limitado a emitir comunicados para anunciar adhesiones de miembros (uno de los más mediáticos fue Microsoft), y un limitado número de análisis del estado de la técnica, por contra no han realizado tan apenas propuestas.

La última propuesta en llegar ha sido Thread Group (Thread Group 2015) avalada por Google (Google 2015c) tomando como base el caso de éxito de Nest (una de sus empresas más relevantes en IoT). Cuenta entre sus socios a empresas como Samsung, ARM, Freescale y Qualcomm además de numerosos afiliados. Thread se presenta como una propuesta de protocolo de comunicaciones, muy centrado en conectar dispositivos del hogar. Se anuncia como sencillo, eficiente y seguro. Basado en el estándar 6LoWPAN (IPv6 sobre 802.15.4), la mayor parte de los chips que implementen ZigBee podrán usar Thread. Desde el consorcio no se descarta su adaptación para que sea aplicable a otras tecnologías de comunicación como Bluetooth y WiFi.

Por otro lado, parece que tanto Google como Apple están tratando de ofrecer sus propias propuestas de IoT, si bien es cierto, que ambas lo hacen desde un enfoque aún más centrado en Internet que en las Cosas. Así por ejemplo el actual Airplay (Apple 2015a) de Apple podría entenderse como el primer acercamiento a los estándares para IoT, idea que se ve potenciada con la presentación en 2014 de HomeKit (Apple 2015b) , un *framework* para conectarse y controlar diferentes accesorios del hogar. Por su parte Google acaba de anunciar su protocolo Weave como una capa de comunicación universal, integrada en su nuevo sistema operativo Brillo (Google 2015a) basado en Android y orientado a conseguir la interoperabilidad entre dispositivos (incluso entre aquellos que no utilicen Brillo).

Los organismos de estandarización, son figuras transversales, sin intereses propios preconcebidos, que tratan de armonizar el contexto técnico existente para fijar unos acuerdos comunes. Con

respecto a IoT, cabe mencionar la propuesta IEEE P2413 (IEEE 2015) que pretende definir la arquitectura de un *framework* para IoT, con una perspectiva global. Abarca desde la definición formal de las diferentes capas y elementos, la abstracción de los mismos y sus relaciones, hasta propuestas de documentación y armonización de estándares. Todo ello manteniendo un espíritu integrador, siguiendo la idea de un modelo de referencia para definir las relaciones entre los diversos mercados verticales de IoT y los elementos comunes de la arquitectura. Se prima la simplicidad para el desarrollador, puesto que contempla aspectos como la abstracción de datos, la seguridad, protección, etc. Aunque el número de miembros adscritos no es elevado (actualmente 24) cabe destacar que entre ellos se encuentran tanto Qualcomm (líder de facto de AllSense) e Intel (su homólogo para OIC). Esta es una de las iniciativas que más expectación mantiene, pues se espera que desde el IEEE se repita el éxito de propuestas previas, como las del grupo IEEE802.15 para las WPAN (con protocolos tan asentados como 802.15.1 Bluetooth y 802.15.4 Zigbee), o el IEEE802.11 con Wi-Fi. El Internet Engineering Task Force (IETF) es otro organismo de normalización que está trabajando en la estandarización de protocolos para la IoT (Zhengguo Sheng et al. 2013). Sus propuestas se articulan en torno a RPL (*Routing Protocol for Low Power and Lossy Networks*) (Winter 2012) y CoAP (*Constrained Application Protocol*) (Shelby 2012). No obstante, parece que su impacto real en el ámbito de IoT es menor, quizás por tratarse de una visión muy centrada en las capas superiores.

Junto a esas grandes alianzas, surgen otras entre empresas de menor calado (oneM2M, ISA100). De igual modo es posible encontrar comités, organismos y alianzas (OASIS 2015), (IPSO Alliance 2015), que realizan actividades de vigilancia tecnológica, difusión e incentivación de IoT. Algunos organismos tienen carácter gubernamental (como la Comisión Europea) que realizan revisiones continuas del estado de la cuestión (European Commission 2015b) y promoción de proyectos como “Alliance for Internet of Things Innovation” (AIOTI) (European Commission 2015a) y “Digital Single Market” (European Commission 2015c).

Una de las mejores vías para convertir una propuesta en el estándar de facto, es la adopción mayoritaria por parte de los desarrolladores. Los desarrolladores, suelen sentir afinidad por plataformas y herramientas abiertas, que les permitan una mayor productividad, que ofrezcan soporte, y dispongan de una amplia comunidad, abundante documentación y ejemplos de libre uso (West, Gallagher 2006). Hasta el momento, solo la alianza AllSeen ofrece estas facilidades a los desarrolladores, de modo que ya empieza a ser una alternativa tenida en cuenta por los mismos. Por otro lado tanto IEEE P2413 como Thread están generando gran atención. El primero por venir propuesto por la IEEE Standards Association y el segundo por estar basado en propuestas ampliamente conocidas y aceptadas (ZigBee y 6LowPan) y avalado por importantes empresas.

1.1.2 ARQUITECTURA DE IOT

La IoT es un concepto complejo que abarca distintos entornos, desde el más físico y tangible a través de las Cosas hasta el más virtual con la abstracción de las mismas en Internet. Por ello, IoT suele ser expuesto desde varias perspectivas (Singh, Tripathi & Jara 2014): la visión desde Internet, considera los servicios, los datos en la nube, las comunicaciones IP (Internet Protocol), etc.; la visión desde las Cosas (Thiesse, Michahelles 2010), como elementos físicos que son, estudia aspectos como redes de sensores, interfaces de usuario, consumo; por último existe una aproximación desde el punto de vista más abstracto, que se centra en el conjunto y considera la construcción de IoT a partir de sus ontologías (Wang et al. 2012), semánticas (Barnaghi et al. 2012) y otras aproximaciones al conocimiento (Wang et al. 2013b). Por ello el número de tecnologías implicadas en IoT son elevadas. Para realizar una descripción desde una perspectiva técnica del concepto de IoT, se suele realizar una segmentación de la misma en varios niveles (Perera et al. 2014a). Existen diferentes visiones, pero de modo general se podría hablar de los siguientes niveles: Cosas, redes de Cosas, aplicación y servicios (Bandyopadhyay, Sen 2011). Los dos primeros tienen por objetivo, llevar el mundo real al virtual, y los dos siguientes son los responsables de manipular la información y generar servicios a partir de ella. Entre estos mundos se encontraría Internet, como medio para interconectar el mundo real y el virtual. A continuación se describen estos niveles, exponiéndose un esquema de los mismos en la Figura 1:

- Las Cosas (nivel Cosas) están integradas en el mundo real con objeto de extraer información e interactuar con él y con las personas. Están sujetas a una serie de restricciones físicas, y sus capacidades son limitadas, puesto que son los elementos más tangibles de todo el sistema.
- Las Cosas con características comunes (principalmente tecnología de comunicación) se agrupan (nivel redes de Cosas) en un subconjunto al que en ocasiones se denomina NoT (Network of Things) (Gubbi et al. 2013), (Asensio et al. 2014). En un mismo espacio pueden coexistir múltiples NoT. Generalmente la comunicación entre Cosas de una misma NoT es directa; entre Cosas de distintas NoT (suele implicar un cambio de tecnología de comunicación) se requiere un elemento que haga de adaptador, el Gateway. En la situación actual de IoT, el Gateway es un elemento fundamental que tradicionalmente se presenta como el medio de conexión a Internet. De este modo, el Gateway es el encargado de facilitar la interconexión entre NoT (con lo que no se necesitará acceder a los niveles superiores), gestionar cada una de las NoT, e incluso implementar cierto nivel de inteligencia y procesamiento local.
- Una aplicación (en la nube y/o local) se encarga de gestionar la información asociada a las diferentes NoT. Esta aplicación establece una serie de conexiones con un conjunto de *Gateways* (cada uno de los cuales puede gestionar varias NoTs) que en general comparten una misma finalidad o ámbito de aplicación.

- En un momento dado se puede requerir implementar un servicio, pero sin preocuparse del origen de la información o de los aspectos más físicos del proceso, para ello se utilizará las interfaces de conexión a diferentes aplicaciones, integrando y procesando la información de multitud de fuentes.

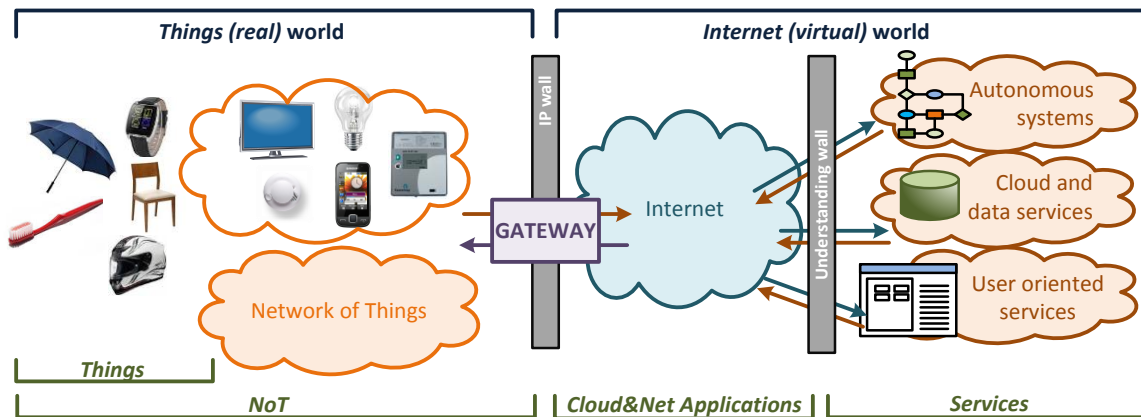


Figura 1: Niveles en IoT

A continuación se propone el ejemplo de un servicio para mejorar la eficiencia energética del parque de viviendas de una ciudad (basado en los desarrollos realizados en el marco de esta tesis para el proyecto Reinassance), que trata de condensar lo anteriormente expuesto. La descripción se realiza desde los niveles inferiores. En cada hogar particular podrán existir varias NoT, por ejemplo:

- Sensores de temperatura, humedad y electroválvulas en radiadores, con comunicación ZigBee formarán una NoT con capacidades de sensado y actuación.
- Varios *SmartMeter* integrados en cada línea eléctrica de la casa y en los enchufes conformarían una NoT de elementos comunicados vía PLC por ejemplo.
- Una red WiFi en la que estarían la TV, el PC y un número variable de *smartphones*, constituirían una tercera NoT.

Cada piso dispone de un *Gateway* que gestiona las 3 NoTs anteriores, y las conecta a Internet. Un sensor de temperatura al sobrepasar cierta consigna, podría actuar sobre una electroválvula directamente y de modo autónomo (mostrando así cierto nivel de inteligencia) al estar en la misma NoT.

El nivel de confort actual se podría consultar en un *smartphone* gracias a que el *Gateway* interconecta las diferentes NoT implicadas, y realiza un procesamiento inicial de la información para determinar el confort a partir de los sensores de temperatura y humedad. El usuario desde su televisión, podrá ajustar los umbrales de confort. Para una vigilancia remota del hogar por parte del usuario, los datos serán empaquetados y enviados a Internet a través del *Gateway*.

En el centro de control del edificio, una aplicación recogerá la información de cada uno de los *Gateway* de los pisos, y podrá gestionar algunos parámetros. Cada *Gateway* no enviará la información desagregada y en tiempo real, por considerarse algo privado, sino que la enviará procesada y filtrada. Igualmente desde la aplicación de control no se podrá realizar cualquier acción de control. Por ejemplo no estará permitido encender el radiador de un piso, aunque si se podrá enviar una consigna de potencia eléctrica máximo total requerida, que no podrá ser sobrepasada.

A nivel institucional, se plantea realizar una iniciativa para incentivar la eficiencia energética. Para ello, en el centro de control de la ciudad, se implementa un servicio de monitorización diaria del consumo energético. Este servicio, agrega la información proveniente de distintas aplicaciones, como las de gestión de edificios privados, alumbrado público, predicciones meteorológicas, etc. Con estos datos, se podrá realizar unas encuestas, e informar a cada usuario, de su posición en el ranquin y ofrecerle directrices para mejorar.

Nótese, como la arquitectura presentada, permite tanto la interacción local directa entre las Cosas (sin necesidad de recurrir a niveles superiores) como la interacción con una Cosa desde un nivel superior (Internet). En cada caso se definen unos permisos de interacción posibles y en general, cuanto más alto es el nivel en el que nos encontramos, el nivel de abstracción es mayor.

1.1.3 LAS COSAS EN IOT

Como se pone de relevancia con las iniciativas anteriores, la estandarización de IoT se suele abordar desde el ámbito de Internet con un enfoque abstracto del problema, propio del mundo software centrado en datos y servicios. Los trabajos en el marco de esta tesis, se van a realizar con una visión integradora, pero desde un punto de vista de las Cosas.

Las Cosas en IoT deben de tener una amplia conectividad y recursos de computación, siendo lo más común tratar de conectarlas a Internet siguiendo los paradigmas web actuales. Diferentes trabajos investigan y categorizan los diversos tipos de Cosas, según su naturaleza y relación con IoT (Kranz, Holleis & Schmidt 2010). Mientras el enfoque más alto de IoT habla sobre ubicuidad, invisibilidad de elementos o context-awareness; desde el enfoque de la Cosas, la atención se centra en aspectos como disponibilidad energética, conectividad continua, interoperabilidad, precio o dimensiones (Kortuem et al. 2010). Aun con todo, no debe perderse de vista que hoy por hoy Internet tiene un esqueleto cableado, que inevitablemente está ahí, además de que en algún momento las Cosas deben ser accesibles desde el mundo IP. Esto supone que en algún punto de la arquitectura de IoT se tendrán que seguir usando los puntos de acceso o *Gateways* para unirse a las infraestructuras cableadas propias de la red de redes. Las Cosas para

formar parte de un escenario IoT, requieren ciertas capacidades en función de su finalidad, y entre éstas, las más comunes son:

- Autoidentificarse y disponer de un identificativo único.
- Ubicarse en el entorno, tanto temporalmente como espacialmente.
- Reconocer su estado. Disponer de mecanismos para conocer características de su propio estado (como nivel de energía remanente, consumo, chequeo de fallos, etc.).
- Conocer el entorno y actuar sobre él.
- Interaccionar con las personas a través de diferentes tipos de interfaz.
- Interactuar con otras Cosas, lo que implica la necesidad de comunicación con las mismas.
- Ser capaz de tomar decisiones o computar, en función de variables externas e internas sobre la forma de comportarse o interactuar.
- Procesar de modo conjunto y distribuido con otras Cosas del entorno.

Esto conlleva contemplar una serie de aspectos tecnológicos, como son:

- Gestión energética, especialmente en relación con los elementos de almacenamiento de energía (baterías y supercondensadores), y en el diseño de cara a la eficiencia energética.
- Comunicaciones, principalmente inalámbricas de bajo consumo.
- Microprocesadores, primando principalmente el consumo energético, el tamaño, coste y las prestaciones de computación.
- Tecnología de sensado y actuación. Los elementos de sensado son múltiples y variados. Al referirnos a actuadores se está considerando los elementos de control próximos a la electrónica y no tanto el automatismo final (así, una puerta automática controlada vía Bluetooth desde otro dispositivo, el elemento de actuación sería la salida digital, el SSR o relé que actúa sobre el mecanismo eléctrico, y no tanto el motor del mecanismo).
- Algoritmia, técnica de procesamiento e inteligencia distribuida.

TECNOLOGÍAS PARA EL DISEÑO DE LAS COSAS

Desde el punto de vista de una Cosa como un dispositivo electrónico, el microprocesador (tanto su aspecto hardware como firmware) es el núcleo de la misma, siendo las comunicaciones el siguiente bloque más importante. A la hora de diseñar Cosas, se debe tener en cuenta que los recursos de sus componentes electrónicos se encuentran limitados (Sehgal et al. 2012), por lo que resulta de interés conocer la situación actual de los aspectos mencionados.

Comunicaciones

La tecnología de conexión requerida para las Cosas vendrá determinada por múltiples factores técnicos, pero simplificando, se puede decir que dependerá de los requisitos de movilidad, cobertura, consumo energético, y ancho de banda.

Los requisitos de movilidad y el área de cobertura, son los primeros factores limitantes. Si el dispositivo no necesita moverse, podrá ser cableado, aunque esto generalmente lleva asociado un mayor coste en la instalación del dispositivo. No obstante, esta opción solo se selecciona cuando se requieren anchos de banda muy elevados (routers), con los dispositivos críticos de una infraestructura (*Gateway*) o cuando se deben utilizar tecnologías de comunicación cableadas por otros motivos (PLC, fibra óptica, alto consumo energético, etc.). Si el dispositivo debe ser móvil o no es posible cablear, necesariamente las comunicaciones deben ser inalámbricas. En la práctica, se considera que las Cosas de IoT se comunican entre sí mayoritariamente de modo inalámbrico. Diferentes trabajos revisan las distintas tecnologías de conexión de las que se puede hacer uso según las diferentes necesidades (Andreev et al. 2015).

En numerosos escenarios, el área de trabajo del dispositivo se restringe a una zona limitada (por ejemplo un edificio, una parcela agrícola, etc.). Estos escenarios han sido ampliamente tratados en el ámbito de la investigación de WSN. Implican el uso de tecnologías que conforman las llamadas redes WLAN (*Wireless Local Area Network*) representadas principalmente por WiFi (Tozlu et al. 2012), y las redes WPAN (*Wireless Personal Area Network*) con ZigBee (Baronti et al. 2007) y BLE (*Bluetooth Low Energy* o Smart, de menor consumo que el clásico) (Gomez, Oller & Paradells 2012) como ejemplos más representativos. Estas tecnologías de comunicaciones permiten desplegar un área de cobertura (en ocasiones en base a una red mallada) con unas distancias de enlace de decenas (WPAN) a cientos de metros (WLAN) permitiendo que elementos inalámbricos (móviles o estáticos) puedan dar el paso a Internet. Diferentes trabajos ponen de manifiesto la necesidad de seleccionar la solución más apropiada en cada situación comparándolos en términos de topología de red, cobertura, tasa de datos o consumo de energía (Zorzi et al. 2010).

Para una zona de cobertura más extensa, se requiere una tecnología que permita una amplia cobertura, hablándose de WWAN (*Wireless Wide Area Network*) (Corson et al. 2010). En general se hace uso de tecnologías como WiMAX, satelital, y redes celulares según CDMA, UMTS (GSM/GPRS, 3G, LTE), aunque estas tecnologías suponen un mayor impacto tanto energético como económico. Para los dispositivos que requieran este mayor rango de cobertura, las alternativas actuales son o bien incorporar tecnologías de comunicaciones como las antes citadas al propio dispositivo, (un *smartphone* es un ejemplo típico), o bien apoyarse en otro dispositivo dotado de capacidad de conectividad a una red de mayor rango de cobertura. En este último caso, el dispositivo que crea una subred de dispositivos a los que permite conectarse a la red más amplia, se dice que actúa como hotspot. Casos frecuentes son los *wearables* conectados vía Bluetooth a un *Smartphone*, creando una red BAN (*Body Area Network*), y la reciente proliferación de router MiFi con conectividad 3G o superior.

Recientemente, surge el concepto de LPWA (*Low-Power Wide-Area*), como el de una red inalámbrica con distancia de enlace de cientos e incluso algunos miles, de metros en la que el consumo de los dispositivos es crítico (autonomía de varios años a partir una pila AA), con tasas de transferencia reducidas, que puedan operar desatendidas durante largos periodos de tiempo y con coste económico de conexión reducido. Se podría describir como las redes de telefonía móvil, particularizadas para las Cosas de IoT (Xiong et al. 2015), al estar más adaptadas a las limitaciones físicas (Rathod et al. 2015) de las mismas. Este tipo de redes se despliegan o bien a partir de soluciones integradas, que requieren infraestructuras particulares, como es el caso de Synapse (Synapse Wireless 2015), Weightless o NWave, o bien haciendo uso de infraestructuras de comunicaciones ya existentes como Sigfox (Centenaro et al. 2015). Algunas de las tecnologías soporte, ya llevan un tiempo en el mercado como On-Ramp Wireless (cuyo proveedor ha pasado a denominarse Ingenu desde Septiembre 2015) (Ingenu 2015), aunque otras son de reciente aparición como LoRa (promovido por Semtech) (Semtech 2015). Se prevé (Morrish 2015) que el número de Cosas con esta conectividad va a experimentar un notable aumento en los próximos años hablándose de los 3000 millones de unidades para el 2025, por lo que este sector se está movilizandote notablemente. Así, Sigfox anuncio a principios del 2015 una ronda de financiación de 115 millones de dólares, Huawei adquirió Neul, a finales de 2014, y una alianza se ha formado en torno a LoRa. En Febrero 2015 Vodafone anunció que va a ser el primer operador en dar soporte a la tecnología LPWA para IoT de Huawei (CIoT), y ambos pretenden que la solución sea validada por 3GPP (3rd Generation Partnership Project). En relación a esto en Agosto 2015 GSMA (*Groupe Speciale Mobile Association*) ha anunciado el lanzamiento de Mobile IoT Initiative un proyecto respaldado por 26 compañías líderes entre las operadoras de telecomunicaciones, productoras de chipset y generadoras de servicios (Vodafone, Cisco, Huawei, IBM se encuentran entre ellas). Se trabajará en cooperación con 3GPP, con la finalidad de conseguir estándares comunes y avanzar en el desarrollo de soluciones LPWA a partir de las infraestructuras celulares actuales, centrándose principalmente en GSM y LTE (Long Term Evolution). Estas iniciativas, parecen altamente prometedoras y permitirían el paradigma de IoT de todos los dispositivos conectados directamente a una red global. No obstante aunque esto fuese posible, es de prever que nunca sustituya a los otros tipos de redes, puesto que los requisitos de las Cosas son muy diversos.

Bajo esta perspectiva, algunos analistas (Näslund 2015) piensan que los operadores de redes móviles van a jugar un importante papel en el ámbito de IoT, puesto que tienen una experiencia previa en la conexión de dispositivos abarcando amplias extensiones. Aunque no obstante será necesaria la adaptación del modelo de prestación de servicio por su parte, puesto que se requiere una asignación dinámica de ancho de banda, en el que cada Cosa pueda usar las comunicaciones solo cuando lo requiriese y con un coste económico únicamente proporcional al tránsito de datos. Desde un punto de vista técnico, habría que considerar el carácter heterogéneo de

dispositivos a conectar, y su frecuente naturaleza asimétrica en el flujo de datos (y a diferencia de las personas, que principalmente consumen información, las Cosas actúan fundamentalmente como generadores de datos).

Microprocesadores

Los microprocesadores de las Cosas priman una serie de características sobre otras que han venido siendo tradicionales, como la potencia de cálculo o la velocidad de procesamiento. Para el diseño de las Cosas se prioriza que los microprocesadores sean de bajo consumo, dimensiones reducidas, rango de tensiones de alimentación amplio y único, estables en su ciclo de operación, de coste económico reducido y que sea fácil desarrollar con ellos (Hempstead et al. 2008), (Pesovic et al. 2012). Como otro de los requisitos de las Cosas es incorporar comunicaciones inalámbricas, cada vez son más frecuentes los WMCUs o Wireless MCUs (*MicroController Unit*), dispositivos que pueden definirse como un SoC (*System on Chip*) que integran capacidades de un microcontrolador y módulos electrónicos para facilitar el diseño de un *transceiver* inalámbrico (Char 2015). En función del protocolo de comunicaciones (su capa física principalmente) para implementar un nodo inalámbrico completamente funcional, puede ser tan solo necesario incluir una antena externa, en otras ocasiones se requiere alguna etapa electrónica adicional externa al módulo. Los primeros de estos SoC integraban dos dispositivos (microcontrolador y transceiver) en un mismo encapsulado, es decir existía una cierta separación física entre aplicaciones. Actualmente es más frecuente una mayor integración, en la que existe tan solo una separación lógica (ambas aplicaciones hacen uso del mismo *core* y espacio de memoria).

Acorde con lo anterior, las características técnicas de las últimas propuestas comerciales, se están adaptando para dar mejor respuesta a los requisitos particulares de las Cosas. Por ejemplo, ARM (no es productora, pero sus IP son la base de numerosos dispositivos) cuenta con microcontroladores de la serie Cortex-M orientados para usarse en aparatos finales muy cercanos al usuario, por lo que son ideales para los dispositivos de IoT. Los últimos movimientos de ARM, parecen indicar su intención de posicionarse en este mercado, así en Abril 2015 ha adquirido las empresas Wicentric (soluciones Bluetooth con un stack de muy bajo consumo) y Sunrise Micro Devices (soluciones IP para comunicaciones inalámbricas por debajo del voltio de alimentación) para mejorar su gama ARM Cordio (SoC basado en Cortex-M y hardware específico para Bluetooth Low Energy).

Otra empresa, en principio alejada de microprocesadores de esta gama, como es Intel también tratan de posicionarse. Así, en el “2013 Intel Developer Forum” se anunció Quark, su SoC especialmente diseñado para aplicaciones de IoT, más pequeños y lentos, pero con un menor consumo que sus microcontroladores Atom. Con objeto de reforzar su presencia, Intel ha ofrecido plataformas de desarrollo basadas en este microprocesador, como Intel Galileo, Intel Edison (mismo factor de forma que una tarjeta SD y microprocesador Quark, finalmente

sustituido por un Atom y con un tamaño ligeramente mayor) y recientemente Intel Curie, especialmente dedicada a dispositivos *wearables* (tamaño de una pila de botón). Todas ellas con una relación coste-prestaciones muy destacable, basadas en un SO Linux y certificadas Arduino (con una clara intención de atraer al gran público).

Samsung parece seguir la misma línea. En Agosto 2014 adquirió por 200 millones de dólares Smart Things (startup centrada en productos SmartHome), que ha utilizado como base para anunciar a principios de 2015 “Smart Thing Open Cloud” que ofrece servicios en la nube a través de SAMI (plataforma de intercambio de datos de Samsung). En la misma línea, pero con mayor atención en las Cosas, en mayo 2015, ha anunciado el entorno Artik para el desarrollo de IoT. Se trata de una plataforma abierta compuesta por módulos hardware (3 opciones con diferentes capacidades), software (también Arduino compatible) y servicios *cloud*, para conectar objetos via WiFi, Bluetooth y ZigBee a Internet. No se dispone de información, pero parece que no van a incluir microprocesadores Exynos, sino adoptar arquitecturas ARM adaptadas a los requisitos IoT.

Otra de las grandes empresas en este mercado, Qualcomm, actualmente ofrece su serie más básica, Snapdragon 410 como solución para IoT. En Mayo 2015 su filial Qualcomm Atheros, anuncia dos nuevos procesadores específicamente diseñados para IoT los QCA401x y QCA4531, con soporte Wi-Fi (incluye el stack de varios protocolos), bajo consumo, y aptos para un mercado sensible al coste económico. El modelo QCA401x dispondrá de 800KB de memoria de programa, y periféricos para la conexión directa de sensores y actuadores. El modelo QCA4531 más avanzado, incluirá un entorno Linux/OpenWRT. Ambos tienen preintegrados el framework Allseen Alliance’s AllJoyn, lo que asegura interoperabilidad directa dentro del ecosistema AllJoyn.

Sistemas operativos

A la hora de abordar el diseño del firmware de estos microcontroladores, surgen diferentes estrategias. Dada la creciente complejidad de las aplicaciones, principalmente con la inclusión de protocolos de comunicación inalámbricos, los fabricantes de microcontroladores, han incluido en sus propios IDE, herramientas que simplifican el proceso de diseño. Algunas de las propuestas de estándares previamente comentados también ofrecen librerías genéricas con la definición del mismo.

En ocasiones se opta por diseñar la aplicación sobre un sistema operativo embebido, estos pueden ser genéricos multiplataforma, o propios del dispositivo utilizado, en cuyo caso suelen ser ofrecidos por el propio fabricante (Farooq, Kunz 2011). Dentro del primer tipo, y para microcontroladores de capacidades moderadas, las opciones más comúnmente utilizadas son Contiki (Contiki 2015), TinyOS (TinyOS 2015), freeRTOS (FreeRTOS 2015) y RIOT (Riot

2015). Todos ellos tradicionalmente se han considerado como RTOS (*Real Time Operating Systems*), aunque dadas sus características, sus requerimientos moderados de microprocesador, y que tradicionalmente se han utilizado como soporte para desarrollar el firmware de las Cosas, ahora se presentan como SO para IoT (Baccelli et al. 2013).

Debido a la creciente potencia de los microprocesadores y a la popularidad de los SBC (*Single Board Computer*) de hardware abierto, como Raspberry Pi, Beagle Bone, Odroid-U3, Galileo, MinnowBoard, etc., se han empezado a valorar alternativas de sistemas embebidos más complejos, siendo los denominados Embedded Linux, los más comunes (por ejemplo Raspbian para su uso con la Raspberry Pi o Angstrom Linux para la Beagle Bone). En general, estos SO, pese a presentarse como embebidos, tienden a olvidarse de las limitaciones de los dispositivos comportándose como un SO al uso. Adicionalmente los SBC en los que se ejecutan, son ideales como plataformas de desarrollo, pero no son adecuados para desarrollar Cosas en aplicaciones reales por cuestiones de consumo, factor de forma y coste. En consonancia con esto, otras alternativas como Windows CE, Symbian e incluso Android deben ser consideradas con cautela como SO para aplicar a las Cosas.

No obstante y gracias a las previsiones en el ámbito de IoT, se está asistiendo a la aparición de nuevas propuestas que parecen haberse marcado como hoja de ruta, pensar en los requisitos y limitaciones de las Cosas.

ARMmbed se presentó a finales del 2014 (la versión estable está prevista para la ARM TechCon en Noviembre del 2015) como un SO específico para IoT, diseñado para la arquitectura Cortex-M, especialmente centrado en el bajo consumo, y con soporte para un amplio *stack* de protocolos inalámbricos, anuncia numerosas librerías de soporte, facilidad de uso e integración con otras herramientas de ARM (por lo que el número de dispositivos en los que podrá aplicarse será muy elevado).

En Agosto 2015 se anuncia Windows 10 IoT Core, capaz de ejecutarse en las SBC MinnowBoard (Intel) y Raspberry Pi 2 (ARM), se presenta como un entorno multilenguaje y multientorno, y afirma estar orientado a dispositivos con recursos limitados y mantener acotado el consumo. Soporta AllJoyn, y por lo tanto es de esperar que disponga de una alta compatibilidad con las directrices que proponga AllSeen Alliance.

Como ya se ha comentado Google ha anunciado su SO Brillo basado en Android, aunque aún no se dispone de especificaciones, apuntan a que estará muy orientado hacia las Cosas, siendo capaz de ejecutarse en dispositivos con escasas capacidades (64MB o 32MB de RAM).

En el Huawei Network Congress 2015, se ha presentado LiteOS, que se enmarca dentro de la propuesta “Agile IoT Solution” de Huawei. Se trata de un sistema operativo abierto a todos los

desarrolladores. Con un tamaño de tan solo 10KB, sin necesidad de configuración y capaz de soportar autodescubrimiento y gestión de red, se ha anunciado como una herramienta ideal para desarrollar de modo sencillo y rápido el hardware inteligente que conforma las Cosas de IoT.

INTEROPERABILIDAD PARA LAS COSAS

La interoperabilidad en IoT implica la capacidad de intercambiar datos, entendiendo la información embebida en estos datos, con objeto de que las Cosas sean capaces de interactuar entre sí siendo accesibles desde Internet. Existen pues tres niveles de relación: intercambio de datos (conectividad), intercambio e interpretación de la información (comunicación) y mecanismos de interacción, y un requisito: posibilidad de acceso desde Internet. Los dos primeros niveles implican lo que tradicionalmente se ha entendido por comunicaciones, mientras que el último nivel, la interacción, es más propio de IoT.

A modo de ejemplo, es frecuente encontrar dispositivos de monitorización de actividad personal que suben los datos a Internet a través de un *smartphone*. Para ello es necesario que ambos dispongan de algún tipo de conexión, por ejemplo Bluetooth. Esta conectividad no asegura un intercambio útil de información a no ser que se haya establecido unas reglas de comunicación, generalmente a través de la definición de un protocolo en el firmware del dispositivo y en la app del *smartphone*. Este protocolo, debería estar optimizado, para encapsular fácilmente la información por un *Gateway* (en este caso el *smartphone*), y hacer la información accesible a Internet. Por último, si varios de nuestros dispositivos de monitorización detectan que estamos sufriendo un problema de salud mientras conducimos, pueden optar por interactuar por ejemplo, con el coche mientras conducimos, para que active las medidas preventivas adecuadas.

Tradicionalmente a la comunicación entre dispositivos se le suele definir de modo genérico con el termino M2M (*machine to machine*). Para facilitar la comunicación entre dispositivos se hace uso de los diferentes estándares propuestos en el ámbito de M2M (Chen, Wan & Li 2012). Las primeras comunicaciones inalámbricas surgieron como sistemas H2H (*human to human*), sin embargo con la aparición y desarrollo de las WSN se dinamizaron las comunicaciones M2M inalámbricas. El crecimiento y el esfuerzo de estandarización global al respecto ha sido muy notable (Chang et al. 2011).

En la IoT, el uso de estándares inalámbricos es notablemente superior al de los cableados. Muchos de ellos, como RFID, WiFi, GSM, etc., habilitan la interconexión, por medio de la descripción de las capas inferiores del modelo OSI (*Open System Interconnection*). De este modo las Cosas de una misma red, que comparten el mismo protocolo, son capaces de realizar acciones como la gestión de red, seguridad, interconexión, etc., llegando a permitir el intercambio de datos. Sin embargo si la capa de aplicación no está definida, las Cosas no pueden comprenderse

o interactuar entre ellas, a no ser que previamente haya existido un acuerdo entre los desarrolladores de cada Cosa. Esto es, no existe conocimiento previo, a no ser que se hayan descrito y explicado propiedades y métodos para cada Cosa en documentos *off-line* tipo Datasheet.

Algunas redes de automatización y control como Lonworks, BACnet, Konnex o CANOpen definen cómo los dispositivos están representados en su propia red, siendo el uso de objetos y variables las aproximaciones más comunes. Esta definición se suele abordar desde dos alternativas complementarias. O bien definir un número amplio de parámetros del protocolo muy específicos y conteniendo un volumen de información reducido, o bien definir un conjunto reducido de parámetros más generales pero que requieren mayor cantidad de información para ser descritos. ISA100.11a es un ejemplo del primer caso mientras que WirelessHART lo es del segundo (Petersen, Carlsen 2011).

Por otro lado, estándares como Bluetooth y ZigBee van un paso más allá para garantizar la interoperabilidad, definiendo perfiles y objetos abstractos que describen dispositivos en la capa de aplicación. Bluetooth define una serie de perfiles estándar, por ejemplo manos libres (HFP, Hands-Free Profile), salud (HDP, Health Device Profile), dispositivos de interfaz (HID, Human Interface Device Profile), etc., asociados a aplicaciones verticales. ZigBee no solo define perfiles verticales como automatización del hogar (HA, Home Automation), energía (SE, Smart Energy), cuidados médicos (PHHC, Personal Home&Hospital Care), etc., sino que también hace una definición horizontal, para especificar como los dispositivos deben intercambiar datos de la aplicación, atendiendo a su funcionalidad por medio de la ZCL (ZigBee Cluster Library) (Specification 2008). La ZigBee Gateway Public Application Profile establece cómo los dispositivos deben ser conectados a Internet y proveer servicios. Adicionalmente ZigBee permite la inclusión de cierto nivel de inteligencia distribuida, definiendo cómo se deben coordinar entre sí los dispositivos para construir escenarios, creando asociaciones virtuales (*bindings*) entre dispositivos.

En algunas ocasiones, dos especificaciones se coordinan entre sí para resolver el problema de la interoperabilidad entre ellas. Por ejemplo ZigBee especifica cómo interoperar con BACnet (Hong et al. 2014), sin embargo esto no deja de ser una solución parcial. En general los dispositivos que usan cualquier estándar de comunicación inalámbrico (como ZigBee) no pueden interoperar directamente con otro estándar (como WiFi) a no ser que exista un agregador de protocolos que realice la interconexión entre ambos mundos.

El estándar IEEE1451(Lee et al. 2007) es una especificación no dependiente de la red de comunicaciones, orientada a ser usada con transductores inteligentes, que proporciona un lenguaje común, independientemente del protocolo utilizado. La norma define los diferentes

perfiles de aplicación como medioambiental, medidores inteligentes, monitorización de la salud, automatización inteligente del hogar, control industrial, etc. El estándar se basa en el uso de las llamadas TEDS (*Transducer Electronic Data Sheet*) para describir un conjunto de interfaces de comunicación para la conexión de transductores, microprocesadores, sistemas de instrumentación, redes de control de campo, etc. (Song, Lee 2008a). Según la especificación IEEE1451.0, las TEDS ofrecen información sobre la identificación del transductor, operación, calibración, fabricante, etc. A partir de las especificaciones del estándar IEEE1451.5 para las especificaciones de radio es posible implementar redes de Cosas inalámbricas sobre otros estándares como WiFi, Bluetooth, ZigBee (Higuera Portilla, Polo Cantero & Gasulla Forner 2010), (Fernandes et al. 2013) y hacer uso de estándares orientados a comunicaciones IP, como 6LowPan (Higuera, Polo 2011). De modo similar IEEE1451.2 define comunicaciones cableadas como SPI y UART, IEEE1451.6 sobre CANOpen e IEEE1451.7 sobre RFID. Esta interoperabilidad es conseguida por medio del NCAP (*Network Capable Application Processor*) que agrega los diferentes módulos TIM (*Transducer Interface Module*) sobre el mismo lenguaje común. A través del NCAP y siguiendo IEEE1451 es posible implementar servicios web que pueden hacer a las Cosas descubribles, accesibles y controlables vía Internet (Song, Lee 2008b).

Una vez que está garantizada la conectividad eficiente entre dispositivos, una serie de estándares como XMPP (*Extensible Messaging and Presence Protocol*) (Saint-Andre 2011), EEML (Extended Environments Mark-up Language) (EEML 2015), y propuestas como SensorML (OGC 2015) del OGC (*Open Geospatial Consortium*) o SenseWeb (Microsoft Reserch 2015) de Microsoft se centran en proveer interpretación a los bytes intercambiados, integrando sensores y actuadores en el mundo virtual. Sin embargo, estos protocolos se suelen quedar a nivel taxonomía de la información, y simplemente expresan consultas y modelado de datos, por lo que carecen de la semántica y ontologías que son necesarias para el procesamiento de información compleja. Esto implica que no son del todo aptos para la creación de servicios orientados a los niveles más altos del conocimiento.

Acorde con lo anterior, se requiere de un grado más alto de abstracción del conocimiento. Iniciativas como SENSEI (Presser et al. 2009), COSE (Wemlinger, Holder 2011), DogOnt (Bonino, Castellina & Corno 2008) y otras (Pfisterer et al. 2011) aproximaciones ontológicas en entornos inteligentes, relacionan entre si las Cosas a través de relaciones semánticas e integran éstas sin fisuras con servicios web (Guinard et al. 2010). Este tipo de aspectos se encuentran más próximos al ámbito de Internet que al de las Cosas, y estrictamente no pueden considerarse como protocolos de comunicación. No obstante, para realizar aportaciones sobre los protocolos actuales, es interesante conocerlas para tratar de conseguir el transporte e interacción de la abstracción de la información de modo eficiente y sencillo.

En base a lo anterior, puede comprobarse como no existe un único protocolo que garantice la interoperabilidad entre las Cosas, sino que la solución actual pasa por utilizar estándares en diferentes capas. Las abstracciones de la información en los niveles superiores se encapsulan dentro de los protocolos de comunicación de niveles inferiores. Desde una perspectiva integral, IEEE1451 parece ser una buena opción para IoT, puesto que, además de definir los niveles inferiores de la comunicación, fuerza la definición de las especificaciones tanto de la Cosa como de la propia interfaz de red. Con ello se provee independencia del protocolo de comunicaciones, y se permite además la auto identificación de los dispositivos, la auto documentación y en definitiva capacidades *plug&play*. Estas capacidades permiten simplificar la instalación, actualización y mantenimiento. Sin embargo, este estándar tiene una escasa penetración en el campo de IoT, limitándose su uso prácticamente al campo de la instrumentación electrónica, razón por la cual en la actualidad apenas es compatible con el hardware existente. Esto es debido, principalmente a que los desarrolladores de IoT provienen del campo de las ciencias de la computación (y consideran aplicaciones semánticas), a la propia complejidad de los estándares y/o al excesivo detalle en aspectos electrónicos que no son usados por la aplicación final. Otros estándares de comunicación como ZigBee o 6LoWPAN son mucho más usados en IoT pero implican restricciones a un hardware determinado y en ocasiones no profundizan en la cuestión de interoperabilidad con otras tecnologías, aunque quizás con la iniciativa Thread, esto último tienda a suavizarse.

Accediendo al mundo IP

La complejidad en cuanto a protocolos para IoT, contrasta con la sencillez en Internet. De hecho, su evolución fue posible gracias a la existencia de un protocolo único común, HTTP como mecanismo mínimo de intercambio de información (textos, imágenes, videos, etc.). Posteriormente, otros protocolos (FTP, SMTP, POP, IMAP, etc.), fueron surgiendo como respuestas específicas a otras tareas más concretas. En justicia, se debe mencionar que este tipo de protocolos han funcionado relativamente bien, porque las máquinas que interconectan emplean un vocabulario restringido, poseen unas características físicas determinadas (inicialmente las comunicaciones eran cableadas y sin restricciones de dependencia energética), y una gran homogeneidad en los requisitos de las comunicaciones. (del tipo servidor-cliente basadas en modelos request/response en tiempo real). Pero en el caso de IoT, la naturaleza particular de cada Cosa y su uso, dificulta la existencia de una solución óptima común.

Si se habla de IoT, en algún momento es necesario que las virtualizaciones de las Cosas se muevan a través de Internet, por lo que se deberá hacer uso del lenguaje IP. Gran parte de los estándares de comunicaciones de alto nivel, incluyen IP como una parte de sus especificaciones (aunque como se acaba de ver esto no garantiza la interoperabilidad a nivel de aplicación). Sin embargo, las Cosas son elementos con recursos restringidos e IP no es un protocolo que fuese ideado teniendo en cuenta esas restricciones; por ejemplo las cabeceras sobrecargan notablemente el

mensaje, algo problemático en dispositivos con memoria ajustada, o que necesitan minimizar el tiempo de transmisión. Adicionalmente las Cosas son inalámbricas, por lo que los niveles inferiores de las comunicaciones pueden no soportar la operativa IP, al tener que contemplarse la posibilidad de que el dispositivo no permanezca activo. Por ello es necesario identificar las restricciones y realizar modificaciones sobre IP para disponer de una transmisión de datos eficiente (Rodrigues, Neves 2010). Surgen de este modo diferentes propuestas como CoAP (Castellani et al. 2011), (Patro, Banerjee 2015) y MQTT (MQTT 2015), siendo 6LoWPAN (6LoWPAN 2015) las más conocidas. 6LoWPAN se presenta como un estándar que posibilita el uso de IPv6 sobre redes basadas en el estándar IEEE802.15.4, es sin duda uno de los mecanismos más extendidos para conseguir que las Cosas de una red inalámbrica puedan comunicarse directamente con otros dispositivos IP. De modo simplificado, 6LoWPAN se basa en definir mecanismos de compresión/descompresión de cabeceras, para aligerar IPv6. En general estas propuestas garantizan eficiencia en la continuidad y robustez en la conectividad, pero no proveen semántica. Frecuentemente, en el caso de redes heterogéneas, el mismo *Gateway* que provee conectividad IP hace las veces de agregador, llevando a cabo la traducción entre protocolos a nivel local.

Siguiendo la directriz de 6LoWPAN es posible encontrar diferentes propuestas que permiten encapsular diversos protocolos, por ejemplo Bluetooth (Wang et al. 2013a). De igual modo existen propuestas más complejas, como SNAIL (*Sensor Networks for an All-IP World*) (Hong et al. 2010) que apoyándose en 6LoWPAN y CoAP ofrece una solución que contempla aspectos adicionales como seguridad, habilitación de otros servicios web (TCP, UDP) sincronización y movilidad (estos dos últimos no nativos en IP). Otros trabajos partiendo de 6LoWPan introducen modificaciones con objeto de mejorar su eficiencia y facilitar su aplicación en entornos heterogéneos típicos en la IoT (Jara, Zamora & Skarmeta 2012).

Eficiencia energética

Las aplicaciones de las Cosas de la IoT son muy variadas, por lo que los requisitos tecnológicos que deben cumplir las mismas son muy diversos. Al diseñar una Cosa habrá que tener en cuenta que tendrá que ofrecer servicio en diferentes escenarios de uso y en todos ellos es deseable que esté presente de modo ubicuo, lo que implica dos vertientes, una espacial y otra temporal. La ubicuidad espacial supone la capacidad de ubicar la Cosa en cualquier lugar y en ocasiones permitir su desplazamiento. Esto suele implicar el uso de comunicaciones inalámbricas que no restrinjan la movilidad, lo que limita la posibilidad de una alimentación cableada continua. Por otro lado una ubicuidad temporal supone asegurar la disponibilidad de la Cosa en cualquier momento y durante tanto tiempo como sea posible (idealmente de modo indefinido), de modo que se debe minimizar el consumo del dispositivo. En definitiva, ya sea tanto por la no facilidad de acceso a una fuente permanente de energía, como por la necesidad de extender al máximo la autonomía, la eficiencia energética de las Cosas es algo crítico y prioritario (Anastasi et al. 2009). Las investigaciones en el ámbito de WSN en torno al bajo consumo de los nodos de la red (Sharma et al. 2011), (Popovici, Magno & Marinkovic 2013) son extrapolables al diseño energéticamente eficiente de Cosas, aunque el análisis puede mejorarse teniendo en cuenta consideraciones adicionales (Abbas, Yoon 2015). En esencia una Cosa de IoT es un nodo generalizado de una WSN, y en ambos casos los principales factores que contribuyen al consumo energético son los mismos: las comunicaciones inalámbricas seguidas del consumo asociado al sensado y procesado (Asensio et al. 2013). Cuando una Cosa se encuentra en un entorno real, surgen diversas restricciones relacionadas con su dependencia energética: no hay una fuente energética ilimitada, la energía del ambiente es escasa y no es suficiente para un funcionamiento continuo, el mantenimiento de los dispositivos es problemático (acceso difícil o imposible para cambiar las baterías), etc.

La energía requerida para operar una Cosa deber ser tan pequeña como sea posible, y su optimización necesita un conocimiento multidisciplinar y se debe abordar desde una perspectiva combinada (Rault, Bouabdallah & Challal 2014). Se deben considerar tanto aspectos propios de las redes de comunicaciones (distribución espacial de los nodos, control de acceso al medio, algoritmos de enrutamiento...) (Sendra et al. 2011), (Chabarek et al. 2008) como consideraciones aplicables al diseño del nodo (Gao, Fan 2006). En el diseñado de una solución IoT, suele existir mayor capacidad de decisión y diseño en el lado de las Cosas puesto que generalmente en el despliegue de redes comerciales se utilizan soluciones *mainstream* sobre las que se tiene menor control (a excepción de utilizar una tecnología diseñada ad-hoc). Es por ello que el diseño hardware (Yu, Qinghua & Xiyuan 2010) y firmware (Park, Lee 2008) del nodo son cruciales, aunque sin embargo con demasiada frecuencia, es realizado de modo superficial. En ocasiones la optimización energética se limita a recopilar los requerimientos de los diferentes

bloques hardware y optimizando parcialmente el código firmware (Salvadori et al. 2009), y todo ello pese a que existen numerosos trabajos que ofrecen diferentes estrategias y consejos para abordar el diseño de un dispositivo con comunicaciones inalámbricas de modo eficiente (Asensio et al. 2013), (Rabaey et al. 2006), (Arabi 2014), (Shearer 2011).

Para realizar un diseño energéticamente eficiente, se tiene que conocer previamente y del modo más exacto posible el consumo del dispositivo. Esto implica no solo su valor medio, sino también su distribución a lo largo del tiempo, e incluso las demandas pulsadas de energía (comunes durante el proceso de comunicación inalámbrica) (Martinez et al. 2015). Adicionalmente, un diseño óptimo, requiere disponer de estos consumos de modo desagregado, tanto para cada uno de los bloques hardware como para las distintas rutinas de procesamiento en el firmware. Es posible encontrar distintos modelos de consumo y estrategias de análisis del mismo. Este análisis no solo es útil en la fase de diseño (Yu et al. 2014), sino que también es deseable durante la propia operación del dispositivo (Merentitis et al. 2012), para disponer de información más realista.

La obtención de energía del entorno, o *harvesting* energético (Vullers et al. 2009), (Harb 2011) es el proceso por el que se recolecta energía de una fuente del entorno, se procesa y almacena para su uso futuro por el dispositivo (Sudevalayam, Kulkarni 2011). Este tipo de tecnologías se han venido usando en el ámbito de las WSN, para el diseño de nodos energéticamente independientes (Mathúna et al. 2008), (Alvarado et al. 2012). Las fuentes de energía que comúnmente han sido más utilizadas son: lumínica (Dondi et al. 2008), térmica (Tan, Panda 2011), eólica (Sardini, Serpelloni 2011), cinemática (Szarka, Stark & Burrow 2012), movimiento humano (Mitcheson et al. 2008). En estos sistemas, la elección de la tecnología de almacenamiento y su arquitectura (batería única, o múltiples baterías), es también un importante factor a analizar (Knight, Davidson & Behrens 2008).

1.1.4 MÉTRICAS EN IOT

Como con cualquier otra tecnología, con IoT se requiere una evaluación objetiva de la solución implementada. Aunque existen algunas propuestas para la IoT (Gluhak et al. 2011) y otras previas provenientes del ámbito de la WSN (Bhuyan et al. 2010), (Xia 2008) esta problemática no se ha tratado con gran profundidad. Evaluar la calidad de una implementación IoT no es trivial puesto que es un sistema amplio y complejo, basado en una tecnología muy heterogénea y cuyo resultado es algo abstracto que puede ser altamente dependiente tanto de la implementación final del servicio generado como del uso que se le dé a la propia IoT.

Para ello, se recurre al concepto de métrica como el de un indicador que cuantifica, de acuerdo a una definición previa, alguna característica determinada. Las métricas pueden indicarse de

manera absoluta respecto a una cualidad, o relativa para relacionar dos características. Las métricas relativas más frecuentes son las relacionadas con la medición del factor de calidad de servicio (*QoS Quality of Service*) en las que como en cualquier medición de eficiencia se mide los resultados conseguidos frente a los costes requeridos. En ocasiones también se pueden expresar en términos de rendimiento como una relación entre el comportamiento actual y un resultado máximo previamente estimado.

Los QoS no solo tienen utilidad para evaluar la implementación de un sistema, sino que también son la base de los mecanismos de detección de errores. Cada vez son más frecuentes los sistemas que incluyen mecanismos de autoevaluación. En esencia se trata de que los propios sistemas realicen una auto monitorización de un conjunto de métricas de modo periódico, para detectar cualquier desviación de las mismas respecto de unos valores previamente considerados adecuados. Este enfoque puede darse tanto a un nivel más centrado en la Cosa (*Yang et al. 2015*), como más global, considerando también la parte de comunicaciones (*Razzaque et al. 2014*). En el caso más avanzado, puede utilizarse para definir la calidad del servicio que se está prestando, a la que algunos trabajos se refieren como calidad de control (QoC, Quality of Control) (*Pozalujan et al. 2015*), para indicar de modo genérico que se define la calidad de una acción de control como la diferencia entre unas consignas de entrada y el resultado alcanzado.

Como IoT está constituida por diferentes subsistemas, se suele analizar por separado cada uno de los mismos, siendo en el ámbito de las comunicaciones donde más se ha avanzado en la definición y uso de métricas (*El-Sayed et al. 2008*), (*Uthra, Raja 2012*). Su uso es muy común en la investigación relacionada con las WSN donde existe un amplio consenso en utilizar algunas métricas. Entre ellas, se encuentran desde indicadores absolutos de características como el ancho de banda, throughput, tasa media de errores, tiempos de acceso, latencia de datos, etc., hasta métricas más complejas que tratan de evaluar de un modo global la efectividad en la transferencia de datos, incorporando simultáneamente varias de las variables anteriores (*Xiong et al. 2014*). En ocasiones algunas de las capas de los protocolos de comunicación (generalmente en los aspectos más relacionados con acceso al medio y enrutado) incluyen en sus especificaciones directrices de métricas (*Del-Valle-Soto et al. 2014*) acordes con sus propios requisitos. En los casos anteriores, se aplica un enfoque muy centrado en evaluar la calidad de la red de comunicaciones, aunque con la aparición de IoT, se empieza a dar una versión más integradora a las métricas (*Forsström, Österberg & Kanter 2012*) considerando que las comunicaciones no son solo el fin sino el medio.

De igual modo, centrado en el ámbito de los dispositivos, se suelen utilizar diferentes métricas del consumo de los mismos (tratadas en el punto anterior en modo de eficiencia energética). Las más comunes son el consumo medio para un ciclo tipo de operación definido, y la energía consumida en cada fase de ese ciclo. De igual modo, resulta frecuente el uso de métricas y otros

mecanismos de medición de calidad en el ámbito del software. No obstante, este último aspecto de IoT no es objeto de esta tesis.

Si bien las métricas de aspectos concretos de IoT son de utilidad, el desempeño de IoT debería ser evaluado en conjunto, no a partir de un aspecto particular de su estructura (Duan, Chen & Xing 2011). Para ello, conviene analizar cuáles son los resultados y cuáles son los costes. Tanto unos como otros se pueden enfocar desde una perspectiva local (aplicada por ejemplo a una determinada Cosa), desde un punto de vista centrado en la infraestructura de las NoT (Cosas, routers, Gateway...) o incluso desde un enfoque global que considera IoT como sistema (acceso a internet, servidores, servicios en la nube...)

En el ámbito de IoT, es frecuente referirnos a los siguientes costes:

- Costes energéticos: suele aplicarse una visión local desde la Cosa, considerándose solo la energía consumida por ella. No obstante en ocasiones puede ser necesario un análisis global. Por ejemplo, enviar un dato a Internet será energéticamente más costoso si se hace mediante un dispositivo con tecnología GSM que con uno en una red ZigBee. Pero en el segundo caso habría que tener en cuenta, el consumo de los posibles routers intermedios, el *Gateway*, etc.
- Coste económico: puede resultar complejo de analizar puesto que hay una parte fija (coste de las propias Cosas), otra variable (el tránsito de datos y la propia energía de operación suelen llevar asociado un coste económico). Por otra parte hay que definir como se repercuten los costes ocultos del resto de los elementos que sustentan la infraestructura de comunicaciones.

La identificación de resultados en IoT es complicada, ya que un sistema IoT no está concebido para ofrecer un único servicio concreto o resolver una cuestión determinada. Por eso las métricas de efectividad en IoT se suelen particularizar para un servicio u objetivo determinado. Para ello se asume que en esencia, el objetivo final (incluso para la prestación de un servicio) de la IoT, implica un intercambio y/o manipulación de información, algo que es más cuantificable.

Actualmente no es común encontrar estándares de métricas globales en el ámbito de IoT, aunque comienzan a aparecer propuestas que integran distintos niveles, como la sensorización, comunicación y aplicación (Li, Li & Zhao 2014). En general, una vez implementada una aplicación IoT, los propios desarrolladores del sistema, suelen definir sus propias métricas (Paschou et al. 2013), (Jin et al. 2012), (Chen et al. 2011) como forma de relacionar alguno de los resultados buscados por su IoT frente a alguno de los costes como los previamente comentados y la tecnología involucrada (Liang et al. 2013).

1.1.5 RETOS DE IOT

Muchas de las tecnologías anteriores, se encuentran lo suficiente maduras por separado como para considerar que las soluciones IoT son abordables. No obstante todavía existen una serie de barreras que vencer antes de la generalización de IoT (Karimi, Atkinson 2013), (Harrop, Harrop & Das 2015), algunas de ellas no solo técnicas:

1. Conectividad a Internet: Internet no es ubicua, existen numerosas áreas del mundo en la que no hay cobertura; de modo simplificado se presentan dos retos:

- Países no industrializados, sin apenas infraestructuras de comunicaciones: Se investigan comunicaciones de larga distancia, baja tasa de datos, económicas y robustas, para prestar servicios mínimos.
- Países desarrollados con infraestructuras de comunicaciones pero con zonas de sombras de cobertura: Se investigan procedimientos para conectar de modo económico y rápido a las infraestructuras ya existentes.

Grandes empresas como Cisco, Huawei, Google (Google 2015b) y otras están trabajando en alternativas generalmente de tipo WiFi de menor coste y consumo energético que el actual.

2. Reducido número de dispositivos con verdadero potencial de uso: Aunque existen un gran número de dispositivos electrónicos en el entorno, la mayor parte de ellos aún no están conectados a Internet, ni a ningún otro tipo de red. Incluso en el caso de que estén conectados a Internet, el intercambio de información con ellos en ocasiones no es posible.

3. Escalabilidad compleja: Las soluciones actuales son válidas para un número de dispositivos acotado. Hacer despliegues extensos suele ser costoso y, en ocasiones, las infraestructuras, tanto de comunicación como de procesado de información, no están dimensionadas para manejar un número ingente de nodos. Un incremento drástico del número de dispositivos conectados a Internet requerirá incrementar capacidades de la red, así como el ancho de banda neto y el número de direcciones (aunque gracias a IPv6 parece que esto último no será problemático).

4. Necesidad de compartir datos de todos los objetos: El éxito de IoT pasa por la compartición de datos y la interoperabilidad entre dispositivos, para eso aparte de superar una serie de problemas técnicos (Borges Neto et al. 2015) se debe concienciar a:

- Los fabricantes de dispositivos, que deben adoptar un mismo protocolo y dejar accesibles sus dispositivos.
- A los explotadores del modelo de negocio, que deben poner énfasis en generar utilidades reales, compartición de datos, y no bloquear el acceso a los recursos a otros explotadores.
- Los desarrolladores deben usar nuevas herramientas, capaces de manejar de forma abierta y eficientemente volúmenes de datos no imaginados hasta la fecha.

5. Estandarización del “conocimiento”: No existe una representación estándar del “conocimiento”, e incluso su propia representación es complicada. Aun en el caso más sencillo, como el de una característica física, ésta puede inferirse con diferentes sensores que utilizan diversas unidades, codificaciones, desviaciones, etc., que dificultan una estandarización. Tampoco existen unas directrices o consenso sobre en qué nivel se debe llevar a cabo el procesamiento de la información, si en el dispositivo, en la red, o en servidores centrales. Desde disciplinas como la inteligencia artificial se ha venido avanzando en esta área con conceptos como ontología de la información y taxonomía de datos.
6. Fragmentación del Mercado: Desde el punto de vista de los desarrolladores de componentes electrónicos, va a ser complicado ofrecer un chip que pueda ser integrado en todos los dispositivos. Algo que tradicionalmente sí era posible en otros segmentos (por ejemplo el número de transceivers GSM/GPR es reducido, y compartido entre un gran número de móviles).
7. Problemas de compatibilidad en los protocolos de comunicación: Es uno de los grandes problemas actuales, aunque las Cosas estén conectadas, no son capaces de establecer un diálogo inteligible entre ellas por la falta de estándares comunes.
8. Seguridad y protección: Tanto para proteger los datos que se obtienen (principalmente los que sean de carácter personal, como los generados por los dispositivos wearables) como la seguridad e integridad del propio sistema (un sencillo ataque con inhibidores de frecuencia puede dejar totalmente inoperativa una red inalámbrica, y desbaratar una importante parte de IoT asociada).
9. Necesidad de selección y adopción de nuevos lenguajes de programación, sistemas de integración y plataformas más idóneas entre el elevado número de alternativas actuales. Los desarrolladores de aplicaciones IoT deben ser conscientes de ambas vertientes: Datos y Dispositivo y aunque se centren en una de ellas, realizar el diseño de modo que se facilite el trabajo a los desarrolladores de la otra vertiente, seleccionando por ello herramientas que permitan esta versión integradora (Hodges et al. 2013), (Hamblen, van Bekkum 2013).
10. Falta de experiencia previa y diversidad de enfoques en el diseño: Por un lado existe una falta de conocimiento sobre lo que es IoT, lo que permite, y sus capacidades futuras. Por otro lado, las personas involucradas en el desarrollo actual suelen tener enfoques muy centrados en el ámbito de la disciplina de la que provienen (desarrollo web, procesado de datos, diseño electrónico, comunicaciones inalámbricas...) y proponen soluciones desde su enfoque parcial. Todo ello a la larga puede suponer una implementación sesgada y no universal de IoT (Kortuem et al. 2013).

11. Todos los dispositivos requieren energía para funcionar: Es necesario disponer de baterías, y/o fuentes de alimentación, que aseguren un funcionamiento prácticamente indefinido del dispositivo. Sin duda pese a ser un concepto trivial, es uno de los principales escollos para el avance de IoT.

Si se agrupan estos motivos, se puede considerar, que las causas que dificultan la implantación de IoT pueden ser de la siguiente naturaleza:

- Técnicas: Tiene que existir una tecnología soporte que permita la implantación. Los aspectos técnicos más críticos y restrictivos actualmente son:
 - Asegurar una autonomía energética de los dispositivos.
 - Resolver la interoperabilidad entre los dispositivos.
- Económicas: Debe existir un beneficio económico, que incentive a las empresas, el interés actual se focaliza en el uso de los datos, principalmente creando conciencia de modelos de mercado que los ponga en valor.
- Sociales: Los servicios prestados tienen que aportar algo de utilidad, con unas características deseables (seguridad, privacidad, acceso universal, etc.) y tienen que ser demandados. Los aspectos más restrictivos actualmente son:
 - Privacidad, se genera el problema ético-legal de la pertenencia y uso de los datos.
 - Seguridad y mantenimiento de IoT, o como asegurar que siga prestando servicio ante fallos no intencionados o deliberados.

Se debe incidir, en que estos requisitos son escalonados pero a la par conjuntamente necesarios. El aspecto técnico, obviamente es el básico (si no existen respuestas técnicas, no se darán los siguientes pasos). El mayor reto en este sentido consiste en conseguir consenso dentro de la multitud de alternativas (se estima que el número de protocolos para IoT supera los 450), o el de cómo conseguir que fluya la información. Pero aunque se resolviesen todos los aspectos técnicos, si no se consigue primero un beneficio económico y una aceptación social, IoT no llegará a ser una realidad.

La presente tesis se centra en realizar aportaciones en relación con algunos de los siguientes requisitos técnicos, en concreto, en las problemáticas asociadas con la optimización energética y la interoperabilidad de las Cosas.

1.2 DESCRIPCIÓN DEL TRABAJO DE TESIS

1.2.1 ORGANIZACIÓN DE LA TESIS

La presente tesis doctoral está presentada como compendio de publicaciones según el acuerdo del 20 de Diciembre de 2013 del Consejo de Gobierno de la Universidad de Zaragoza, por el que se aprueba el Reglamento sobre tesis doctorales. De acuerdo con esta regulación, este documento consta de las siguientes partes:

- **Resumen.** Página inicial en la que se especifica que la tesis es un compendio de publicaciones.
- **Autorización de los directores** para la presentación de la tesis en esta modalidad y el informe motivado de la Comisión Académica responsable del programa de doctorado.
- **Capítulo 1, Introducción** (presente capítulo). En él se realiza una introducción general al objeto de la tesis, seguida de una exposición sobre el estado del arte. Finalmente se incluye un apartado en el que se describe el trabajo de tesis, indicando su motivación, objetivos investigadores, y la metodología de realización en la que se presentan los trabajos y se justifica su unidad temática.
- **Capítulo 2, Manuscritos.** Como resultado del proceso investigador, se han generado diferentes resultados científicos. Una copia de cada publicación se proporciona en este capítulo, indicándose en el Apéndice 1 las características bibliográficas de los mismos. En Apéndice 3 se indican participaciones en resultados relacionados con el ámbito de la tesis. Los manuscritos que conforma la tesis son los siguientes:

- **Manuscrito 1 (Diseño HW):** “Hardware Architecture Design for WSN Runtime Extension”.

Contiene la base teórica de las aportaciones a la optimización energética para dispositivos de IoT. El problema está abordado desde una perspectiva local y física de las Cosas centrado en su hardware y ciclo de trabajo considerando a la misma del modo más genérico posible (esto es, como un nodo de una WSN).

- **Manuscrito 2 (IoT Energy Awareness):** “Energy-awareness application for the Internet of Things”

Investiga las tecnologías soporte (comunicaciones, alternativas Gateway, diseño Cosas, etc.), evolucionando una aplicación tradicionalmente resuelta con WSN (Wireless Sensor Network) a un sistema IoT, con lo que se ofrece respuestas a problemas previos no resueltos y nuevas capacidades. El despliegue de la solución requiere el diseño de Cosas (en este caso diversos nodos sensores), con unos requisitos (amplio periodo de operación) que impactan en sus restricciones de consumo. Por ello resulta crítica la aplicación de las conclusiones presentadas en “Manuscrito 1”.

- **Manuscrito 3 (Interoperabilidad):** “Protocol and Architecture to Things Into IoT”

Contiene la base teórica para las aportaciones a la interoperabilidad para dispositivos de IoT, se expone el concepto de CTP (*Common Things Protocol*) como propuesta de protocolo con un enfoque distinto para conseguir la interoperabilidad entre las Cosas. Se aborda el problema de cuantificación objetiva de los resultados, proponiéndose una serie de métricas para comparar CTP frente a otras propuestas.

- **Manuscrito 4 (Smart Signal):** “Managing Emergency Situations in the Smart City”

Se investigan las capacidades de IoT en el ámbito de la ciudad, y cómo, cualquier dispositivo (en este caso una señal) puede convertirse en una Cosa de IoT adquiriendo con ello nuevas capacidades y ofreciendo nuevos servicios. Asegurar la interoperabilidad al implementarse sistemas complejos con dispositivos heterogéneos y no típicos es un reto, por lo que en este trabajo se aplican y evolucionan los resultados de “Manuscrito 3”.

- **Manuscrito 5 (WSN Traffic):** “Wireless Sensor Networks in Traffic Management Systems”

Junto a la heterogeneidad de los dispositivos que conforman una IoT, otro de los grandes retos, ya expuesto en “Manuscrito 4”, es el despliegue de la misma en grandes áreas. Este trabajo avanza al respecto y propone el concepto de u-Cloud, como un mecanismo de solución. Se aborda el uso de IoT en un nuevo ámbito (gestión de tráfico) estrechamente relacionado con aspectos abordado en “Manuscrito 4” (*Smart Signal y Smart City*) lo que nuevamente requiere aplicar los resultados previos (eficiencia energética e interoperabilidad).

*A cada manuscrito se le ha asignado un nombre descriptor breve (entre paréntesis), para facilitar su posterior referencia.

- **Capítulo 3, Conclusiones y trabajo futuro.** Presenta los principales resultados obtenidos en la tesis, agrupados según los objetivos planteados inicialmente. Se incluye las futuras líneas de investigación a partir de los resultados alcanzados.
- **Capítulo 4, Apéndices.** Compuesto por cuatro apéndices:
 - Apéndice 1. Características bibliográficas de las revistas en las que se han publicado los manuscritos del capítulo 3.
 - Apéndice 2. Renuncia de los coautores no Doctores a presentar los trabajos de los que son coautores como parte de otras Tesis.
 - Apéndice 3. Participación en otros resultados relacionados en el ámbito de la tesis.
 - Apéndice 4. Visión económica y social de IoT.
- **Referencia Bibliográfica,** incluye el listado de las referencias bibliográficas citadas en el presente documento.

1.2.2 MOTIVACIÓN DE LA TESIS

La realización de la presente tesis doctoral, enmarcada dentro del grupo de investigación HOWLab del Instituto de Investigación en Ingeniería de Aragón, presenta una doble motivación. Por un lado, la investigación en el ámbito de IoT y por otro, ofrecer soluciones a las necesidades en proyectos de investigación activos. Desde el grupo de investigación se considera estratégico la adquisición de conocimiento en el ámbito de IoT, por lo que se ha apostado por la investigación al respecto. Así, junto a la presente tesis se están desarrollando otros trabajos de tesis en el ámbito de IoT que exploran aspectos complementarios como el diseño de servicios, *harvesting* energético, redes de sensado en entornos amplios, etc.

La participación en diversos proyectos por parte del doctorando ha supuesto algunos retos tecnológicos que han motivado la investigación en los aspectos tratados en la presente tesis. Entre estos proyectos, cabe destacar:

- Proyecto Renaissance: Renewable Energy Acting In Sustainable and Novel Community Enterprises (Iniciativa CONCERTO 6º Programa Marco europeo).
El objetivo fue evaluar y definir mecanismos de ahorro de energía dentro de comunidades vecinales principalmente a través del estudio del comportamiento social por medio de las TICs. IoT se presentó como una herramienta de gran utilidad para la captura y análisis de información, y su posterior transmisión a la persona en forma de directrices de comportamiento.

- Proyecto Liga Energética (Financiado por la Universidad de Zaragoza). Consistió en diseñar, desarrollar y desplegar un sistema de monitorización ambiental y energética en Edificio de I+D del Campus Rio Ebro de la Universidad de Zaragoza para concienciar a los usuarios sobre el uso de energía y los mecanismos de ahorro. Su realización supuso poner a prueba las capacidades de IoT para aglutinar dispositivos heterogéneos y agrupar la información extraída de los mismos para generar un servicio. Se abordó el diseño de Cosas (dispositivos de sensado ambiental y consumo eléctrico), en las que los requisitos de eficiencia energética eran de vital importancia.

- “Desarrollo de un sistema de señalización de seguridad controlado por sensores en diversos entornos” (financiado por el programa de apoyo I+D+i de la Diputación Provincial de Zaragoza a la empresa innovadora).

En colaboración con la empresa Implaser, el objetivo fue dotar de inteligencia a señales informativas, de manera que su mensaje se adapte automáticamente de modo óptimo a las condiciones de su entorno. Este proyecto, supuso un punto de inflexión en las líneas de investigación del grupo de investigación. Tras su ejecución se optó por aplicar el modelo de Cosa a dispositivos no considerados hasta el momento y la aplicación del paradigma IoT a sistemas de señalización y gestión de tráfico.

- “Sistema inteligente de señalización de emergencia en túneles” (financiado por el Plan para Incentivar la I+D+i en las Empresas de la Provincia de Zaragoza, y las Ayudas para el Desarrollo Competitivo de la Actividad Industrial en Aragón).

En colaboración con la empresa Implaser, se aplicó el modelo de Cosa a las señales tradicionales, dotándolas de capacidades de sensorización, comunicación y procesamiento de la información, para diseñar sistemas de señalización con funcionamiento autónomo e inteligencia distribuida.

- MovVI: Movilidad Verde Inteligente (cofinanciado por el Ministerio de Economía y Competitividad-RTC-2014-2425-4).

Su objetivo principal es desarrollar sistemas IoT que presten servicio en la Smart City, para mejorar la gestión del tráfico y los aparcamientos. Los principales retos a abordar son la heterogeneidad de dispositivos, la adversidad del entorno y el área de despliegue a cubrir.

- SigueTu: Sistema de Guiado de emergencia en Túneles (cofinanciado por el Ministerio de Economía y Competitividad RTC-2015-3359-4).

A partir de la señalización inteligente se pretende diseñar un sistema autónomo, capaz de ofrecer la mejor ruta de escape en una situación de emergencia en un entorno tan complicado como un túnel, y guiar a los cuerpos de emergencias. La eficiencia energética, estabilidad de operación y conectividad entre subsistemas son algunos de los retos tecnológicos a abordar.

Desde la perspectiva científico-técnica, el desarrollo de esta tesis está estrechamente relacionado con algunas de las líneas de investigación troncales del grupo de investigación, en concreto:

- Hardware: Tecnologías de sensado y procesamiento de la señal, diseño electrónico eficiente y de bajo consumo, redes inalámbricas de sensores y actuadores y comunicaciones estándar.
- Sistemas inteligentes embebidos: Middleware para la conectividad del hardware y comunicaciones con el software y el modelado y representación del conocimiento.

El estado del arte pone de manifiesto el gran potencial de IoT, existiendo al respecto una amplia y dinámica investigación, desarrollo e implementación de resultados. De igual modo, la interdisciplinariedad de las tecnologías involucradas hace que se trate de un campo de trabajo, activo con novedades y aportaciones continuas. IoT se trata de un concepto tecnológico en el que existe no solo un gran interés académico, sino también empresarial, social e institucional. Aunque existen publicaciones técnicas y tesis centradas en el ámbito de IoT, la mayor parte se realizan desde una visión de muy alto nivel que obvia que las Cosas no son entes abstractos, sino reales y por lo tanto tienen unas limitaciones. Algunos de los principales retos actuales para conseguir la evolución de IoT son debidos a estas limitaciones. Por ello, la presente tesis viene motivada por la posibilidad de ofrecer soluciones a algunos de los retos en la evolución de la IoT, abordando dos aspectos intrínsecamente relacionados con las Cosas, como son su eficiencia energética e interoperabilidad.

Las descripciones de IoT a la hora de referirse a las Cosas, utilizan términos como ubicuidad o autonomía, algo que es imposible de alcanzar si existe una dependencia energética que debe ser satisfecha. Toda propuesta que mejore la autonomía de cualquier dispositivo electrónico energéticamente dependiente es de utilidad por sí misma. Esto es aún más crítico en el caso de las Cosas de IoT, en donde una de las premisas básicas, es que pasen desapercibidas, algo que no es posible si periódicamente tenemos que sustituir sus baterías. Esta reposición energética resulta económicamente costosa, complicada o imposible de llevar a cabo. Tómese como ejemplo una de las aplicaciones IoT presentadas en la tesis, el sistema de señalización de emergencia en túneles, en donde no resulta sencillo el acceso a los dispositivos una vez instalados, toda vez que implicaría un acceso a la vía interurbana con tráfico. Este hecho motivó tratar de realizar aportaciones que ayudasen a mejorar la eficiencia energética de las Cosas para minimizar su dependencia energética. Se pretendió avanzar en el ámbito de la modelización energética de las Cosas, y poder proponer estrategias de diseño hardware y gestión firmware que mejorasen la eficiencia.

Frecuentemente se dice que IoT supondrá la interacción entre los objetos que nos rodean. Junto al requisito de que las Cosas pasen desapercibidas, su operación tiene que ser desatendida. Así,

cuando una nueva Cosa se introduce en un entorno, debería ser capaz de interoperar con las que ya se encuentran en él de modo inmediato. No obstante esto no suele ocurrir, puesto que aun para conectar dos dispositivos de tecnologías similares pero distintos fabricantes, se requiere algún paso de vinculación o configuración previa por parte del usuario (a no ser que sigan un estándar de amplia difusión). Así por ejemplo, vincular vía Bluetooth el teléfono con la radio del coche, cada vez es más sencillo, pero no es igual de inmediato conectar ese mismo teléfono a cualquier televisión (pese a la cada vez mayor presencia de las SmartTV). Si esto último es complicado, distamos aún más de que cuando llegemos a un edificio, los sensores distribuidos en el mismo informen a nuestro móvil de las condiciones ambientales y situación del mismo. Justamente un escenario similar se trató de avanzar en otra de las aplicaciones de IoT mostradas en esta tesis. Por ello, facilitar la interoperabilidad entre las Cosas que conformarán IoT ha sido otra de las motivaciones de la presente tesis.

Sin ser uno de los objetivos inicialmente implícitos a la hora de iniciar la investigación en el ámbito de IoT, tan pronto se realizaron propuestas e implementaron soluciones IoT, se puso de manifiesto la necesidad de disponer de mecanismos que cuantificasen y comparasen las ventajas de los resultados alcanzados frente a otras alternativas. Se revisaron las métricas y/o factores de calidad que se venían aplicando en otras áreas (especialmente comunicaciones), pero se comprobó que ninguna de ellas era completamente satisfactoria. Ello motivó la investigación en la definición de mecanismos que permitiesen la evaluación del desempeño de IoT como un todo.

1.2.3 OBJETIVOS DE LA TESIS

El objetivo principal de la tesis consiste en realizar contribuciones a la implementación práctica de IoT, principalmente a la interoperabilidad y a la optimización energética de los dispositivos que forman parte de Internet de las Cosas.

Para ello los objetivos parciales, formulados como aportaciones que se pretende alcanzar con el desarrollo del trabajo de tesis son:

1. Revisión del estado del arte de IoT.

Por un lado se revisan las arquitecturas propuestas para dar soporte a la implementación de un sistema de IoT. Por otro lado se consideran las capacidades actuales de las tecnologías involucradas en el desarrollo de Cosas de IoT. Esta revisión transversal, permite identificar las funcionalidades que se desean de las Cosas que conforman IoT y poner de manifiesto las necesidades y requisitos que afectan a las mismas.

2. Aportación a la modelización de las Cosas como un elemento esencial de IoT.
Como elemento básico que constituye IoT, es de interés disponer de una abstracción o modelo de la Cosa. Este modelado se realiza desde el punto de vista de las capacidades, interacciones, y necesidades del elemento esencial conformador de IoT. El modelo se propone con una visión integradora tras la revisión del estado del arte, realizando una aproximación tecnológica, que considera la Cosa como un sistema electrónico. Este enfoque permite concretar y contextualizar las aportaciones posteriores.
3. Aportación al *energy awareness* y bajo consumo de las Cosas.
Se pone de relevancia que las Cosas como elementos reales que son, están sujetas a unas limitaciones físicas, y se incide en que la ubicuidad de un dispositivo, pasa por garantizar su independencia energética. Para avanzar en este aspecto, el primer paso es definir una metodología para el análisis del consumo energético de las Cosas, acorde con el modelo propuesto, y basado en su estrategia de uso. A partir de esta metodología, se evalúan las diferentes estrategias de diseño, tanto a nivel de arquitectura hardware como a nivel de gestión de la Cosa. En concreto se investiga la arquitectura SoC (*System on Chip*) frente a las dual (microcontrolador y *transceiver*), y se analiza el impacto sobre el consumo total de los diferentes estados (principalmente rutina de sensado) del ciclo de operación.
4. Aportación a los mecanismos de interoperabilidad entre las Cosas.
En primer lugar se identifican y definen los requisitos e implicaciones de la interoperabilidad entre dispositivos. Se revisan los mecanismos, protocolos y estrategias actuales sugeridas para garantizar la interoperabilidad entre las Cosas, identificándose las fortalezas y debilidades de cada propuesta. Este análisis se complementa con los resultados de los puntos anteriores (modelado de la Cosa y requisitos deseables). A partir de esta información se propone una alternativa para facilitar la interoperabilidad de las Cosas.
5. Diseño, desarrollo e implementación de sistemas que integren las aportaciones anteriores.
Se aborda el desarrollo e implementación de sistemas que den servicio a necesidades y proyectos reales. Estos sistemas se utilizan como herramientas de demostración, validación, y generación de información para las fases de rediseño y como elementos base para continuar la investigación en IoT.
6. Aportación a los mecanismos de análisis y evaluación de los sistemas IoT.
A la hora de dar respuesta a una necesidad a través de una implementación de un sistema IoT pueden existir distintas alternativas tecnológicas. Cada una de ellas tiene sus ventajas y limitaciones, por lo que resulta de utilidad disponer de mecanismos de comparación. Por ello, se definen métricas y mecanismos que resulten de utilidad para cuantificar los resultados

del desempeño del sistema; tanto como herramienta de comparación entre alternativas, como evaluación de estado del propio sistema. Se aplican estos mecanismos de análisis y evaluación a las implementaciones de IoT llevadas a cabo.

1.2.4 METODOLOGÍA DE LA TESIS

La metodología seguida en la evolución de la tesis, ha venido marcada por las motivaciones de la misma y la participación en proyectos que hacen uso de IoT para ofrecer un servicio. De este modo pueden distinguirse cuatro fases temporales en las que se han llevado a cabo diferentes hitos:

- Fase 1: Propuesta de una visión de IoT centrada en las Cosas.
 - H1: Revisión del estado del arte.
 - H2: Análisis de arquitectura IoT.
 - H3: Propuesta de arquitectura IoT y modelo de Cosa.
- Fase 2: Identificación de aspectos de mejora y aportaciones en referencia a la eficiencia energética.
 - H4: Análisis y aportaciones para la optimización energética en las Cosas.
 - H5: Diseño de sistemas IoT: Energy Aware System (Renaissance y Liga Energética).
- Fase 3: Identificación de aspectos de mejora y aportaciones en referencia a la interoperabilidad.
 - H6: Análisis y diseños de protocolo de interoperabilidad entre Cosas.
 - H7: Propuesta de métricas
 - H8: Diseño de sistemas IoT: *Smart Signal* (Sistema de señalización inteligente en túneles y SigueTU), y gestión de tráfico (MoVVI).
- Fase 4: Análisis de resultados e implementación.
 - H9: Conclusiones. Redacción tesis.
 - H10: Aplicación de resultados en proyectos activos
 - H11: Trabajo Futuro.

Debe comentarse que las Fase 2 y Fase 3, no son estancas ni completamente consecutivas, sino que en ocasiones han evolucionado a la par. Si bien, es cierto que el aspecto de la eficiencia energética se abordó antes que el de la interoperabilidad, a lo largo de las diferentes implementaciones prácticas (H5) y (H8) se tuvieron ambos aspectos en cuenta. Para clarificar la temporización de la etapa investigadora, a continuación se expone una breve exposición cronológica:

Fase 1: 2012 (Q4)-2013 (Q1-Q2).

En las fases finales del Proyecto Renaissance se colaboró en el despliegue de una WSN para la medida de variables ambientales en domicilios particulares. La necesidad de nuevas capacidades, motivaron el interés en IoT, como mecanismo para ofrecer un servicio más óptimo y avanzado, por lo que se realizó la revisión del estado del arte (H1) y (H2) al respecto, y se concluyó con la propuesta de una arquitectura (H3) capaz de satisfacer los requisitos impuestos.

Fase 2: 2013 (Q3-Q4) – 2014 (Q1).

La participación en el proyecto “Liga Energética” implicó la necesidad de diseño de dispositivos energéticamente eficientes (H4) y (H5) capaces de satisfacer unos determinados criterios de autonomía. Tener que integrar diversos dispositivos, tanto de diseño propio, como comerciales de empresas variadas, motivo la investigación en el ámbito de la interoperabilidad entre Cosas (H6). Los resultados principales de esta fase investigadora se reflejan en “Manuscrito 1 (Eficiencia HW)” y “Manuscrito 2 (IoT Energy Awareness)”.

Fase 3: 2014 (Q2-Q4)- 2015 (Q1).

Se formaliza la problemática de la interoperabilidad (H6) en “Manuscrito 3 (Interoperabilidad)”. Se colabora en diferentes proyectos con la empresa Implaser, con objeto de evolucionar los sistemas de señalizaciones tradicionales a sistemas *Smart Signal*, aplicando la estrategia de convertir una señal en una Cosa de IoT. Se toma consciencia de la necesidad de evaluar el desempeño de un sistema IoT por lo que se investiga en las diferentes métricas aplicables a la misma (H7). Las propias necesidades de la aplicación obligan a que estos dispositivos sean energéticamente eficientes e interoperables con otros dispositivos, (H8), recogiendo en “Manuscrito 4 (Smart Signal)” los resultados. A finales de este periodo se inicia el proyecto MovVI, cuya propuesta de arquitectura (H8) se recoge en “Manuscrito 5 (WSN traffic)”.

Fase 4: 2015.

Se fortalecen los desarrollos en el ámbito de la *Smart Signal*, se inicia el proyecto SigueTu, aplicándose las lecciones aprendidas (H9), en los dos proyectos actualmente activos (H10), y se continuará investigando en IoT (H11).

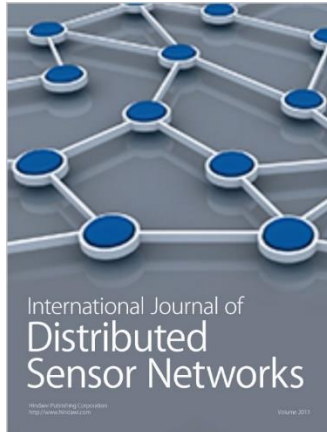
Como en la presente tesis se ha adoptado un enfoque de IoT desde el extremo de las Cosas, se ha realizado el desarrollo de varios dispositivos con funcionalidades diversas, para tratar de analizar las aportaciones realizadas y servir de modelos para futuros dispositivos. El diseño hardware se ha realizado siguiendo la secuencia clásica de diseño. Inicialmente se fijaron sus especificaciones, concretándose conceptualmente mediante sus diagramas de bloques, que a su vez se formalizaron en esquemáticos electrónicos y su correspondiente diseño en PCB. Estos dispositivos se han producido y testeado, entrando en ocasiones en un proceso de rediseño. Se implementó el firmware de los correspondientes dispositivos, siguiendo criterios de modularidad y escalabilidad. El firmware implementado, soporta las capacidades de comunicación inalámbricas conforme al protocolo fijado al efecto. Se investigaron los métodos de estandarización y concreción de firmware que faciliten el desarrollo de futuros dispositivos.

2 PUBLICACIONES

En “Manuscrito 1 (Eficiencia HW)” y “Manuscrito 3 (Interoperabilidad)” se realiza la exposición más teórica y formal de los aspectos de eficiencia energética e interoperabilidad para el diseño de dispositivos de la Internet de las Cosas (IoT), que constituyen el objetivo de la presente tesis. Estos dos artículos muestran las principales aportaciones, como son el modelado de las Cosas, metodología de análisis energético, revisión y contextualización de la interoperabilidad, y propuesta de un protocolo denominado CTP (Common Things Protocol) para mejorar la interoperabilidad anteriormente mencionada entre las Cosas

Como ya se ha comentado, los avances en la investigación se han realizado, en buena parte, motivados por la participación en diversos proyectos en los que el grupo de investigación formaba o aún forma parte. Algunos resultados se plasman en el resto de manuscritos, en los que se aplican y evolucionan los resultados anteriores en desarrollos reales y funcionales de sistemas IoT. Estas implementaciones se enmarcan en diferentes campos, como son los sistemas energy-awareness para el asesoramiento a los usuarios de edificios en “Manuscrito 2 (IoT Energy Awareness)”, la *Smart Signal* en “Manuscrito 4 (Smart Signal)” y la gestión de tráfico viario en “Manuscrito 5 (WSN Traffic)”. En estos trabajos, también se abordan otros aspectos como el diseño electrónico (hardware y firmware) de varias Cosas, la implementación práctica de arquitecturas IoT y la definición de métricas para analizar el comportamiento de IoT.

2.1 HARDWARE DESING FOR WSN RUNTIME EXTENSION



Ángel Asensio, Rubén Blasco, Álvaro Marco, Roberto Casas.
 International Journal of Distributed Sensor Networks
 Article ID 136745, doi:10.1155/2013/136745.

2013

RESUMEN:

El objetivo de la tesis es realizar aportaciones para tratar de minimizar las restricciones que implican algunos de los aspectos físicos de las Cosas. En este trabajo, se aborda uno de ellos, poniendo de manifiesto que la ubicuidad de las Cosas acaba requiriendo su eficiencia energética. Este tipo de problemática, ha sido analizada con profusión en el ámbito de las WSN, pero necesita una revisión para adaptarse al concepto de IoT. Para poder avanzar en el diseño de Cosas energéticamente óptimas un paso previo es tener perfectamente caracterizado su consumo. Por ello, se propone una metodología de análisis que se basa en un modelo de sistema electrónico pero incluyendo su ciclo de operación como una Cosa. Este modelado se realiza desde un punto de vista integrador con dos protocolos de comunicación susceptibles de ser utilizados en el ámbito de la IoT, IEEE1451 y ZigBee, que aunque ofrecen soluciones distintas, ambas cuentan con propuestas interesantes.

A continuación, se consideran distintas arquitecturas de diseño electrónico, analizándose y comparándose el consumo energético de cada una de ellas para distintos casos de uso típicos en el ámbito de la IoT. Se amplía este análisis con otras alternativas y configuraciones, para concluir con una serie de recomendaciones e indicaciones sobre aspectos que, tradicionalmente, pueden pasar desapercibidos a la hora de realizar un diseño energéticamente eficiente para las Cosas.

Research Article

Hardware Architecture Design for WSN Runtime Extension

Ángel Asensio, Rubén Blasco, Álvaro Marco, and Roberto Casas

Institute of Engineering Research (I3A) of the University of Zaragoza, 50018 Zaragoza, Spain

Correspondence should be addressed to Roberto Casas; rcasas@unizar.es

Received 3 August 2012; Accepted 1 April 2013

Academic Editor: Ling Wang

Copyright © 2013 Ángel Asensio et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Internet of Things imposes demanding requirements on wireless sensor networks as key players in context awareness procurement. Temporal and spatial ubiquities are one of the essential features that meet technology boundaries in terms of energy management. Limited energy availability makes anywhere and anytime sensing a challenging task that forces sensor nodes to wisely use every bit of available power. One of the earliest and most determining decisions in the electronic design stage is the choice of the silicon building blocks that will conform hardware architecture. Designers have to choose between dual architectures (based on a low-power microcontroller controlling a radio module) and single architectures (based on a system on chip). This decision, together with finite state machine design and application firmware, is crucial to minimize power consumption while maintaining expected sensor node performance. This paper provides keys for energy analysis of wireless sensor node architecture according to the specific requirements of any application. It thoroughly analyzes pros and cons of dual and single architectures providing designers with the basis to select the most efficient for each application. It also provides helpful considerations for optimal sensing-system design, analyzing how different strategies for sensor measuring and data exchanging affect node energy consumption.

1. Introduction

Internet of Things (IoT) applications and scenarios are very heterogeneous: environmental monitoring in large areas [1], people monitoring in their own homes [2], or industrial environments [3] are some examples. This derives different requirements regarding network architecture and sensing nodes design [4]. According to Merriam-Webster dictionary, ubiquity is defined as the capacity of presence everywhere and in many places simultaneously. Sensors are today needed in different scenarios, and in all of them it is desirable that they be operative everywhere and every time they are required; for this reason, it is said that future sensors must be ubiquitous. It has two faces: spatial ubiquity—which inherently forces wireless communications and absence of wired power sources—and temporal ubiquity—which implies availability along functioning time (maximum energy autonomy) and also availability at any given time. Whichever the case, it leads to the common need of installation's runtime maximization and consequently minimization of energy demanded by sensing nodes [5]. There are many options to power wireless sensor nodes [6], but a real installation usually poses severe

limitations: there is not unlimited power source available, energy from the environment is scarce and not enough for continuous running (e.g., indoors), maintenance of sensors is problematic (e.g., physically hard to reach to change batteries or expensive), and so forth. Thus, is critical to minimize node's power consumption while maintaining application's required quality of service. It is well known that power consumption has a high impact over quality of service offer by a WSN and its lifetime [3–5, 7]; the paper is centered on its analysis.

Depending on the deployment scenario, sensor duties will vary: data sensing, processing, aggregation, forwarding, sending, and so forth. In this paper we focus on a common case in many IoT applications: a sensor node periodically samples (every t_{SAMPLE}) one or more sensors (temperature, humidity, light, presence, chemical concentration, etc.), and then it performs some data processing and reports the readings to the network every t_{REPORT} .

Standard IEEE 1451 describes a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks [8].

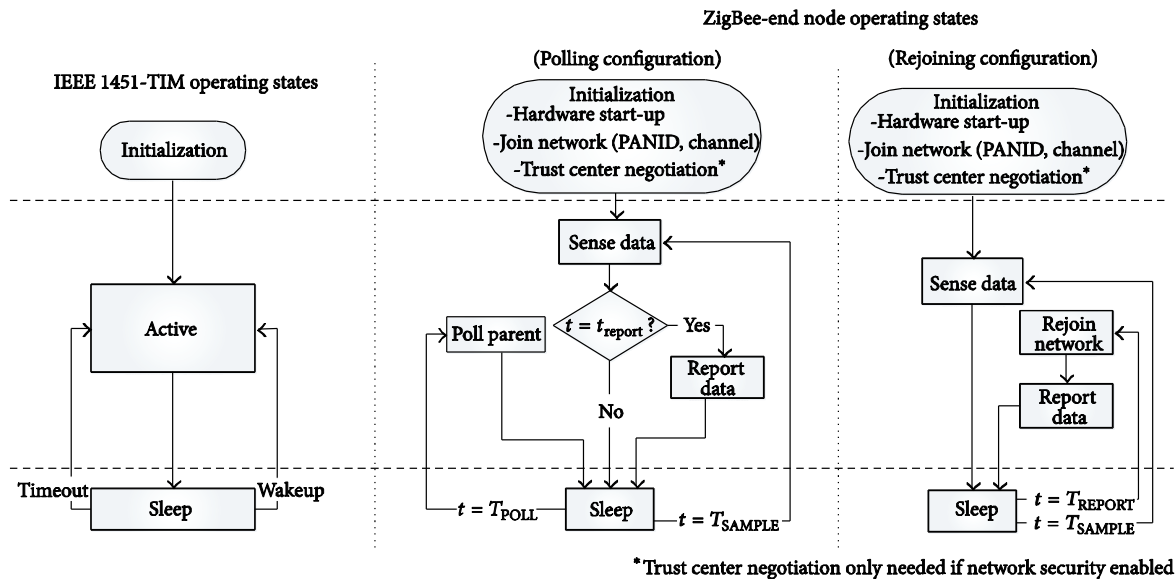


FIGURE 1: Finite state machine that defines a sensing node attending to IEEE 1451 and ZigBee standards.

IEEE 1451 introduces the concept of a transducer interface module (TIM) as a module that contains the interface, signal conditioning, analog-to-digital and/or digital-to-analog conversion, and, in many cases, the transducer. The specification defines a generic finite state machine (FSM) in Figure 1 that describes the operation of sensing nodes—TIMs—with three different operational states: initialization, active, and sleep [9].

IEEE 1451 is not restricted to any communication technology, and thus FSM definition is generic and leaves to each standard the specification of the substates needed. There are many WSN protocols available [10], and we select ZigBee for the study as it is a mature wireless standard for sensor networks, worldwide accepted, and with many hardware manufacturers available. The methodology described could be easily applied to any other standard. According to the standard specification [11], FSM states are defined as follows (Figure 1).

- (1) *Initialization State.* Besides hardware startup (oscillator warmup, peripheral initialization, etc.), the ZigBee node has to initialize the network which means to check its network parameters (PANID—personal area network identifier—and channel mask), and if previously not joined to any network then scan the radio channels to discover available networks, join to a specific network, announce itself in the network, and, if the network has security enabled, wait to be authenticated by the Trust Center and for successful acquisition of the network key.
- (2) *Active State.* Minimum tasks defined are polling its parent (to check if there are messages pending for the node), responding to any device discovery or service discovery operations requested, periodically requesting the Trust Center to update its network key

(if security is enabled), processing device announce messages from other nodes, rejoining the network if disconnected for any reason, searching for alternative parent in order to optimize recovery latency and reliability, and so forth. Besides these network tasks, the node will also manage the sensors it might have, process and send sensor data, and so forth.

- (3) *Sleep State.* It generically does not have any network or sensor and process duty assigned. This state is devoted to power electronics down to the maximum and to wait until there is any task to do switching to active state.

Temporal ubiquity of a wireless sensor node might suppose that communication with node must be guaranteed with a minimal latency time. This is commonly implemented following two different strategies that ensure lowest power of a wireless node: stay connected doing periodical network polls to receive incoming messages or leave the network and periodically reconnect. According to ZigBee specification, this is implemented following two different strategies shown in Figure 1.

- (i) Polling configuration indicates that sensor node never leaves the network and periodically polls its “parent” (another node in the network that holds its messages while it sleeps).
- (ii) Rejoining configuration indicates that sensor node leaves the network between reporting periods.

Both strategies are considered in ZigBee standard but no one is always more convenient than the other; while the first strategy guarantees that the node will receive messages from the network every time it polls, the second strategy reduces radio power consumption between reports to the minimum.

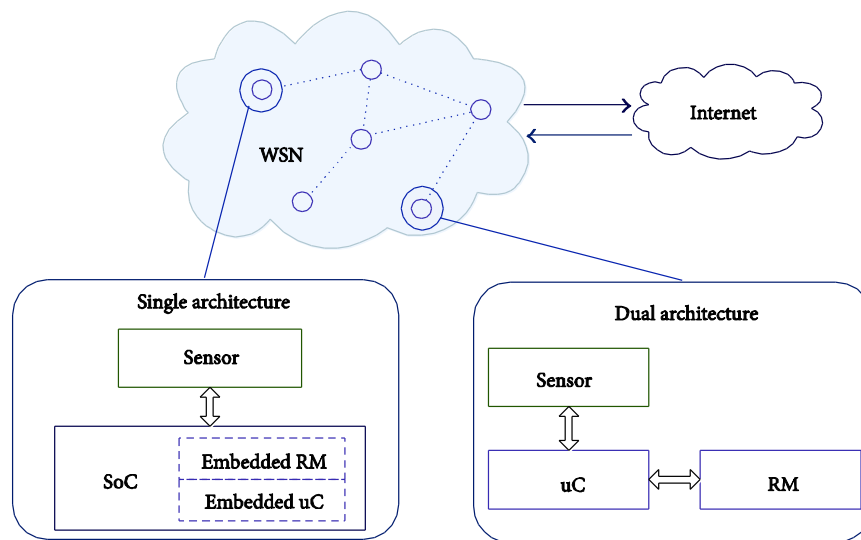


FIGURE 2: Sensor node's single and dual hardware architecture.

Energy required to retrieve and send data from the sensor to its destination must be as small as possible and its optimization needs from a multidisciplinary knowledge are improved electronic stages, network management optimization, cooperative tasking, or other alternatives [12]. It should be approached from a combined perspective [13] that merges network, (spatial distribution of network nodes [14], medium access control [15], routing [16], etc.) and node design considerations. Hardware [17] and firmware [18] design of the sensing node is crucial and it is usually done in a superficial way, just looking at the power requirements of the different hardware blocks and optimizing firmware [19].

This paper analyses energy issues associated with the different design alternatives. The next section shows main hardware architectures used to build a wireless sensor: single and dual. Then, based on the implementation of the previously described finite state machine, a mathematical model of energy consumption is defined. The energetic impact derived from hardware architecture and runtime pattern is presented in Section 4. Finally, several considerations about how design strategies impact over energy consumption and performance comparison of different WSN platforms are shown.

2. Hardware Architecture

The building blocks of a sensor node are power management, sensor, communication, and control and/or processing. Wireless communications are the power hungriest part in a node [20]; nevertheless, its impact in overall energy demand can be reduced as these systems optimize its use to the maximum. On the contrary, power consumption of the sensor is often lower compared to communications, but it can have larger influence on the overall system performance depending on how the node performs the measuring process (sampling rate, signal conditioning, data acquisition, etc.) [21]. As a consequence, hardware architecture of node is

critical when implementing a real application and electronic designers must decide between two different architectures.

- (1) Dual architecture is composed of a microcontroller (uC) that runs the application and control and a radio module (RM) that implements wireless communication. Depending on the radio module, it can just be a transceiver implementing the lowest ISO/OSI layers of a standard (e.g., TI's CC2420 [22], that is, IEEE 802.15.4 compliant) or implementing a specific wireless standard to the application level (e.g., Ember's EM260 network coprocessor implementing ZigBee stack). Both cases share in common the RM that is not programmed, but is just configured or controlled through Universal Asynchronous Receiver/Transmitter (UART), Serial Peripheral Interface (SPI), or Inter-Integrated Circuit (I²C) protocols [23] using a set of commands provided by the manufacturer.
- (2) Single architecture is composed of a system-on-chip (SoC) embedding a radio module and a programmable microcontroller. In this case, the hardware manufacturer provides wireless standard compliance through an API and/or development environment that the programmer uses and implements the application and downloads it to the SoC. (e.g., Ember's 35x with EmberZNet Pro [24] or TI's CC2530 [25] with Z-Stack).

As seen in Figure 2, both architectures can be used to implement a low power consumption end node. Hardware manufacturers are clearly pointing to single architectures in order to maximize energy efficiency, reduce complexity, easily design, and so forth. Nevertheless, is this always true?, under which conditions?, is the strategy of splitting tasks between two low power microcontrollers more convenient in terms of energy efficiency? [26]. In order to answer

TABLE 1: Power modes per silicon blocks (uC, RM, and SoC).

	Power mode 0 (PM ₀)	Power mode 1 (PM ₁)	Power mode 2 (PM ₂)	Power mode 3 (PM ₃)
Microcontroller	Deep sleep (low power timer running)	Low power (slow oscillator, peripherals interrupts on)	High power (fast oscillator)	Not applicable
Radio module	Deep sleep or powered off	Not applicable	Not applicable	Radio on
System on chip	Deep sleep (low power timer running)	Not applicable	Internal uC high power and radio off	Internal uC active and radio on

these questions, in the following sections we compare both architectures analyzing the energy consumption related to each state first theoretically (Section 3) and then with two real implementations.

3. Runtime Energy Consumption Analysis

Energy monitoring during design and commissioning of a wireless sensor network is challenging. Real measurement in specific nodes is possible [27]; nevertheless, WSN characteristics make it difficult to set nodal energy meters all over the network. Thus, it is common to use tools based on nodes' and networks' models that simulate hardware [28], data traffic [29], and associated energy consumption. As it is of key importance to understand the origin of every nanoamp in order to achieve the lowest power consumption [30] and due to the fact that there are no models that consider the architectures described, in the following we study in depth the energy associated with each substate and transition of the sensing node's FSM described in Figure 1.

Minimization of energy consumption is a tradeoff between strategy chosen, application times between events (t_{SAMPLE} , t_{REPORT} , and t_{POLL}), and hardware architecture. According to this, many authors propose different energy models, most of them differentiating between four silicon modules: microprocessor, transceiver, sensor, and power supply [31]. In this study, as we aim to compare the hardware architectures discussed in previous section, it is not needed to consider sensor and power supply models because both will equally affect the energy balance; for example, whichever sensor(s) we use, they will output a digital serial communication interface (e.g., SPI and I²C) or an analog signal that will be, respectively, digitalized by the uC or the SoC.

The estimation of the power consumption of a sensor node is normally based on determination of each of the operation modes of the sensor [32]. These modes are highly influenced by the communication protocol and system hardware. In Table 1, we specify all the power modes in which a node will work.

Table 2 specifies the power mode in which the hardware (uC, RM, and SoC) of the sensor will be in order to work according to poll configuration scheme in Figure 1. (We use poll configuration as it is the most complex scenario and rejoin configuration eliminates "poll parent" state, and the PM₀ of the RM will be reduced, while PM_{0→x} will increase.) Energy necessary to switch between power modes is not negligible, especially when going from low power to high power [33], thus it is also indicated in Table 2.

Energy consumed in a given state "x" will be the sum of its "m" substates calculated as

$$E_x = V \times \sum_{j=0}^m \int_0^{t_j} i_j(t) dt = V \times \sum_{j=0}^m Q_j, \quad (1)$$

where V is the voltage supply and the second term is the integral of the current consumed i_j and during the time t_j the substate lasts.

Attending to the substates and considering the information that can be measured and extracted from hardware datasheets and application notes, the charge demanded by each state is defined in Table 3, where $I_{\text{UC,RM,SoC}_{0,1,2,3}}$ is the current consumed by uC, RM, and SoC in power modes 0, 1, 2, and 3 respectively, $Q_{\text{UC,RM,SoC}_{0,1,2,3 \rightarrow 0,1,2,3}}$ is the charge drained by uC, RM, and SoC in transitions between corresponding power modes, $t_{\text{UC}_{0,1 \rightarrow 1,2,3}}$ is the time needed by uC to change from modes 0 and 1 to 1 and 2, respectively, $Q_{\text{RM,SoC}_{\text{INIT,REPORT,POLL}}}$ is the charge drained by RM and SoC in network initialization, data report, and parent poll, $t_{\text{RM,SoC}_{\text{INIT,REJOIN,REPORT,POLL}}}$ is the time needed by RM and SoC in respective network process, t_{SENSOR} is the time needed by the sensing entities to sensor a valid measure in their outputs, $I_{\text{UC,SoC}_{\text{ACQ}}}$ is the current needed by uC and SOC for data acquisition from the sensing entities, for example, A/D conversion, $t_{\text{UC,SoC}_{\text{ACQ}}}$ is the time needed by uC and SOC for data acquisition from the sensing entities, for example, A/D conversion, $I_{\text{UC,RM}_{\text{SCI}}}$ is the current needed by uC and RM for data communication via serial communication interface, $t_{\text{SCI}_{\text{REPORT,POLL,POLL_ANSW}}}$ is the times needed to communicate between RM and uC via serial communication interface, and t_{SLEEP} is the time in sleep mode.

As we aim to compare both architectures, many simplifications are possible.

- (i) Terms related to network operations ($Q_{\text{RM,SoC}_{\text{INIT,SEND,POLL}}}$) and power state change ($Q_{\text{RM,SoC}_{0,1,2,3 \rightarrow 0,1,2,3}}$) are equivalent in terms of energy consumption for RM and SoC. (This assumption can be considered as RM and SoC from the same manufacturer share the same radiofrequency hardware, for example, Texas Instruments' CC2520 transceiver and CC2530 SoC or Ember's EM357 coprocessor and EM357 SoC.)
- (ii) Charge needed for network initialization is only consumed once and it is negligible compared to the charge needed by other states and consequently to the charge of the battery (below 0,05% with a 1000 mAh battery).

TABLE 2: Power modes in each substate of a normal operating cycle of a sensing node.

States	Substates	Dual architecture		Single architecture
		UC	RM	SoC
Init network	Scan channels	PM ₀	PM ₃	PM ₃
	Discover networks	PM ₀	PM ₃	PM ₃
	Join network	PM ₀	PM ₃	PM ₃
	Announce node in network	PM ₀	PM ₃	PM ₃
Sense data	Change power mode	PM _{0→1}	PM ₀	PM _{0→2}
	Activate sensor and wait for data ready	PM ₁	PM ₀	PM ₂
	Acquire data	PM ₁	PM ₀	PM ₂
Report data	Change power mode	PM _{0→2}	PM _{0→2}	PM _{0→2}
	Exchange “report-data” command (RM → uC)	PM ₂	PM ₃	—
	Change power mode	PM _{2→0}	PM _{2→3}	PM _{2→3}
	Rejoin network (if not polling periodically)	PM ₀	PM ₃	PM ₃
	Send data to the network	PM ₀	PM ₃	PM ₃
Poll parent	Change power mode	PM _{0→2}	PM _{0→2}	PM _{0→2}
	Exchange Poll event (uC → RM)	PM ₂	PM ₂	—
	Change power mode	PM _{2→1}	PM _{2→3}	PM _{2→3}
	Poll parent in the network	PM ₁	PM ₃	PM ₃
	Change power mode	PM _{1→2}	PM _{3→2}	—
Sleep	Exchange “poll response” (RM → uC)	PM ₂	PM ₂	—
	Change power mode	PM _{x→0}	PM _{x→0}	PM _{x→0}
	Sleep	PM ₀	PM ₀	PM ₀

TABLE 3: Consumption in each substate of a normal operating cycle of a sensing node.

States	Substates	Dual architecture	Single architecture
Init network	Scan channels		
	Discover networks		
	Join network	$I_{UC_0} \times t_{INIT} + Q_{RM_{INIT}}$	$Q_{SoC_{INIT}}$
	Announce node in network		
Sense data	Change power mode	$Q_{UC_0→1} + I_{RM_0} \times t_{UC_0→1}$	$Q_{SoC_0→2}$
	Activate sensor and wait for data ready	$(I_{UC_1} + I_{RM_0}) \times t_{SENSOR}$	$I_{SoC_2} \times t_{SENSOR}$
	Acquire data	$(I_{UC_1} + I_{UC_{ACQ}} + I_{RM_0}) \times t_{UC_{ACQ}}$	$(I_{SoC_2} + I_{SoC_{ACQ}}) \times t_{SoC_{ACQ}}$
	Change power mode	$Q_{UC_1→0}$	$Q_{SoC_2→0}$
Report data	Change power mode	$Q_{UC_0→2} + Q_{RM_0→2}$	$Q_{SoC_0→2}$
	Exchange “report-data” command (RM → UC)	$(I_{UC_2} + I_{UC_{SCI}} + I_{RM_2} + I_{RM_{SCI}}) \times t_{SCI_{REPORT}}$	0
	Change power mode	$Q_{UC_2→0} + Q_{RM_2→3}$	$Q_{SoC_2→3}$
	Send data to the network (rejoin if needed)	$(I_{UC_0} \times t_{REPORT}) + Q_{RM_{REJOIN}} + Q_{RM_{REPORT}}$	$Q_{SoC_{REJOIN}} + Q_{SoC_{REPORT}}$
	Change power mode	$Q_{RM_3→0}$	$Q_{SoC_3→0}$
Poll parent	Change power mode	$Q_{UC_0→2} + Q_{RM_0→2}$	$Q_{SoC_0→2}$
	Exchange Poll event (UC → RM)	$(I_{UC_2} + I_{UC_{SCI}} + I_{RM_2} + I_{RM_{SCI}}) \times t_{SCI_{POLL}}$	0
	Change power mode	$Q_{UC_2→1} + Q_{RM_2→3}$	$Q_{SoC_2→3}$
	Poll parent in the network	$(I_{UC_1} \times t_{POLL}) + Q_{RM_{POLL}}$	$Q_{SoC_{POLL}}$
	Change power mode	$Q_{UC_1→2} + Q_{RM_3→2}$	$Q_{SoC_3→0}$
	Exchange “poll response” (RM → UC)	$(I_{UC_2} + I_{UC_{SCI}} + I_{RM_2} + I_{RM_{SCI}}) \times t_{SCI_{POLL_ANSW}}$	0
Sleep	Change power mode	$Q_{UC_2→0} + Q_{RM_2→0}$	
	Sleep	$(I_{UC_0} + I_{RM_0}) \times t_{SLEEP}$	$I_{SoC_0} \times t_{SLEEP}$

TABLE 4: Figures involved in the calculation of power consumption.

	Dual architecture				Single architecture	
	uC _{PIC}	RM _{Ember}	uC _{TI}	RM _{TI}	SoC _{Ember}	SoC _{TI}
I_0	0.835 μ A	0.4 μ A	0.9 μ A	0.4 μ A	1 μ A	1 μ A
I_1	15 μ A	—	41 μ A	—	—	—
I_2	3.05 mA	6 mA	2.2 mA	3.4 mA	6 mA	3.4 mA
I_3	—	27 mA	—	28.7 mA	27 mA	28.7 mA
I_{ACQ}	1 mA	—	850 μ A	—	1.1 mA	1.2 mA
I_{SCI}	0.5 μ A	200 μ A	0.5 μ A	200 μ A	—	—
$Q_{0 \rightarrow 1}$	15 pC	—	16 pC	—	—	—
$Q_{0 \rightarrow 2}$	0.39 μ C	12.4 μ C	10 pC	51.57 μ C	12.4 μ C	51.57 μ C
$Q_{2 \rightarrow 3}$	—	9.94 μ C	—	40.95 μ C	9.94 μ C	40.95 μ C
$Q_{3 \rightarrow 0}$	—	3.3 μ C	—	13.6 μ C	3.3 μ C	13.6 μ C
$t_{0 \rightarrow 1}$	1 μ s	—	0.4 μ s	—	—	—
$t_{0 \rightarrow 2}$	128 μ s	—	0.4 μ s	—	—	—
t_{ACQ}	4.125 μ s	—	2.06 μ s	—	42.7 μ s	68 μ s
$t_{SCI-POLL}$	16 μ s	16 μ s	8 μ s	8 μ s	—	—
$t_{SCI-POLL-ANSW}$	4 μ s	4 μ s	2 μ s	4 μ s	—	—
$t_{SCI-REPORT}$	34 μ s	34 μ s	17 μ s	34 μ s	—	—
t_{REPORT}	—	8 ms	—	8 ms	8 ms	8 ms
t_{POLL}	—	6 ms	—	6.8 ms	6 ms	6.8 ms

(iii) Current in power mode 0 of uC, RM, and SoC is several orders of magnitude lower compared to power modes 1, 2, or 3.

(iv) Time in sleep mode is several orders of magnitude larger than any other times.

Considering the former simplifications and application times between events (t_{SAMPLE} , t_{REPORT} , and t_{POLL}), the resulting energy balance between dual and single architecture for a given cycle is

$$Q_{CYCLE_{D-S}} = \frac{t_{REPORT}}{t_{SAMPLE}} \times Q_{SENSE_{D-S}} + \frac{t_{REPORT}}{t_{POLL}} \times Q_{POLL_{D-S}} + Q_{REPORT_{D-S}} + t_{REPORT} \times I_{SLEEP_{D-S}}, \quad (2)$$

where

$$Q_{SENSE_{D-S}} = Q_{uC_{0 \rightarrow 1}} + Q_{uC_{1 \rightarrow 0}} + I_{RM_0} \times (t_{uC_{0 \rightarrow 1}} + t_{uC_{ACQ}}) + (I_{uC_1} + I_{uC_{ACQ}}) \times t_{uC_{ACQ}} - Q_{SoC_{0 \rightarrow 2}} - Q_{SoC_{2 \rightarrow 0}} - (I_{SoC_2} + I_{SoC_{ACQ}}) \times t_{SoC_{ACQ}} + (I_{RM_0} + I_{uC_1} - I_{SoC_2}) \times t_{SENSOR},$$

$$Q_{POLL_{D-S}} = Q_{uC_{0 \rightarrow 2}} + Q_{uC_{2 \rightarrow 0}} + Q_{uC_{1 \rightarrow 2}} + Q_{uC_{2 \rightarrow 1}} + (I_{uC_2} + I_{uC_{SCI}} + I_{RM_2} + I_{RM_{SCI}}) \times (t_{SCI_{POLL}} + t_{SCI_{POLL-ANSW}}) + (I_{uC_1} \times t_{POLL}),$$

$$Q_{REPORT_{D-S}} = Q_{uC_{0 \rightarrow 2}} + Q_{uC_{2 \rightarrow 0}} + (I_{uC_2} + I_{uC_{SCI}} + I_{RM_2} + I_{RM_{SCI}}) \times t_{SCI_{REPORT}} + (I_{uC_0} \times t_{REPORT}),$$

$$I_{SLEEP_{D-S}} = I_{uC_0} + I_{RM_0} - I_{SoC_0}. \quad (3)$$

Thus, when $Q_{CYCLE_{D-S}} < 0$, the dual architecture will be more power efficient than the single architecture and vice versa when $Q_{CYCLE_{D-S}} > 0$.

4. Experimental Method and Results

As mentioned above, there are different WSN simulation tools that focus on specific aspects of the network: latency times, bandwidth, collisions, message integrity, and so forth. According to the previous section analysis, we need to focus more deeply on the architecture of the node and associated states, than on the network characteristics. Thus, we used MATLAB suite to model energy consumption of real sensing nodes' hardware and simulate FSM operation.

Comparison between architectures has been done analyzing two real implementations with devices having similar

TABLE 5: Rate of consumption of each substate (considering that $t_{\text{REPORT}} = 8$ hours, $t_{\text{SAMPLE}} = 10$ min, $t_{\text{POLL}} = 4$ min, $t_{\text{SENSOR}} = 10$ ms).

	Microchip-Ember	Texas Instruments
$\%Q_{\text{SENSE}_{D-S}}$	33.707%	32.094%
$\%Q_{\text{POLL}_{D-S}}$	0.773%	0.315%
$\%Q_{\text{REPORT}_{D-S}}$	0.007%	0.002%
$\%(I_{\text{SLEEP}_{D-S}} \times t_{\text{REPORT}})$	65.513%	67.589%

characteristics: both ZigBee standard chipsets and microcontrollers with 16 bit RISC architecture similar to MIPS, power supply ranges, integration of peripherals (ADC, serial communication interfaces, clocks, etc.), and memory capacity. Table 4 shows how theoretical analysis shown in Section 3 is specified for two different implementations of ZigBee standard (Texas Instruments and Ember, but now Silicon Labs) and for two different families of ultralow power microcontrollers (Microchip and Texas Instruments). ($u_{\text{C}_{\text{PIC}}} = \text{PIC24F16KA102}$; $\text{RM}_{\text{Ember}} = \text{SoC}_{\text{Ember}} = \text{EM357}$; $u_{\text{C}_{\text{TI}}} = \text{MSP430F2001}$; $\text{RM}_{\text{TI}} = \text{SoC}_{\text{TI}} = \text{CC2530}$. SoC manufacturers usually allow their devices to operate as RM running a specific firmware. Thus, in order to eliminate hardware dependencies in analysis, we decided to use the same chipset operating in different configurations in both architectures. The indicated energy consumption corresponds to the scenarios in which both architectures have optimized and similar performance: similar peripheral, clocks sources, and power configuration. It is important to remark that internal RTCC in PM_0 has been selected.)

For a given conditions and according to the analysis in Section 3, Table 5 shows the charge difference between dual and single architecture ($\%Q_{X_{D-S}}$) of each substate, expressed in percentage contribution to the normalized total consumption per cycle. On one hand, it highlights the importance of sleeping and sensing processes related to total energy consumption evidencing their importance in autonomy maximization. It also proves the slight differences between chipsets, which together with the fact that information available about power consumption is more profuse for Microchip-Ember configuration leads us to choose it for further analyses.

4.1. Sensing and Reporting. When focusing on measurement process, there are two important tasks: data acquisition and reporting. Figure 3 represents how the power savings ratio (PSR) of the dual architecture versus single architecture (defined as $\text{PSR}_{\text{DSvsS}} = Q_{\text{CYCLE}_{D-S}}/Q_{\text{CYCLE}_S} \triangleq \Delta Q/Q$) varies depending on t_{SAMPLE} , t_{POLL} , and t_{SENSOR} . Values above zero indicate better performance of the dual architecture and vice versa when $\text{PSR}_{\text{DSvsS}}$ is below zero.

It is appreciated that variation in t_{POLL} has reduced impact on $\text{PSR}_{\text{DSvsS}}$. The major effect comes from the variation of the time between measurements (t_{SAMPLE}) and the time needed to have valid sensor signal (t_{SENSOR}) [34]; the more time the node spends in sensing tasks, the more effective the dual architecture becomes. This fact is evidenced

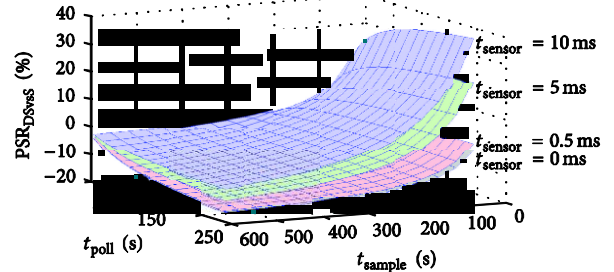


FIGURE 3: Variation of $\text{PSR}_{\text{DSvsS}}$ with t_{SAMPLE} and t_{POLL} (e.g., $t_{\text{REPORT}} = 4$ hours and several t_{SENSOR}).

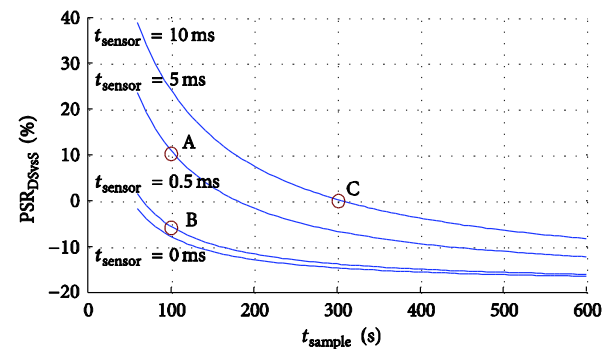


FIGURE 4: $\text{PSR}_{\text{DSvsS}}$ versus t_{SAMPLE} (e.g., $t_{\text{REPORT}} = 4$ hours $t_{\text{POLL}} = 4$ min).

in Figure 4, where $\text{PSR}_{\text{DSvsS}}$ is represented versus t_{SAMPLE} for various values of t_{SENSOR} .

We can clearly observe the impact of the measurement process on energy savings in the following example. Considering a sensor node getting one sample each 100 seconds from a sensor that needs 5 ms to provide a valid value (point A in Figure 3), the dual architecture would need 10% of energy less than single architecture. This effect is mainly derived from the higher flexibility in terms of clock sources of low power microcontrollers that is so far not available in SoCs (PIC24F16KA102 has five external and internal clock sources, providing 11 different clock modes with a minimum CPU clock speed of 31 kHz. Ember 357 has four clock sources with a minimum CPU clock speed of 6 MHz. The same happens to TI's hardware); that is, microcontrollers consider low power modes with slow clocks (PM_1) that are very convenient for sensing tasks. On the other hand if t_{SENSOR} is reduced to 500 μs (point B in Figure 3), single architecture would be 6% more efficient. Finally, when sampling time t_{SAMPLE} exceeds 5 minutes (point C in Figure 3), for the conditions given ($t_{\text{REPORT}} = 4$ hours; $t_{\text{POLL}} = 4$ min; $t_{\text{SENSOR}} \leq 10$ ms), single architecture will be always more efficient.

4.2. Rejoining and Polling Strategies. Regardless of the dual or single architectures, if it is assumable that the node is not connected to the network, a rejoin strategy can be more

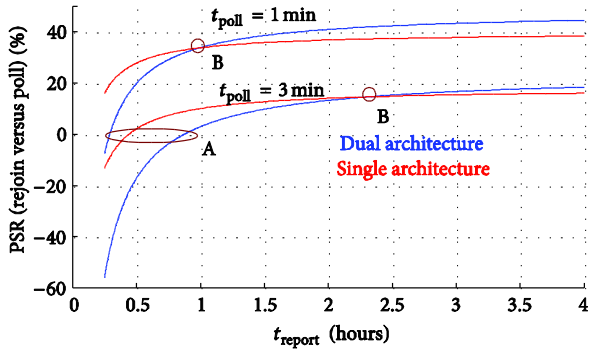


FIGURE 5: Comparison and single dual architecture with rejoining versus polling strategies (example for $t_{SAMPLE} = 1 \text{ min}$ $t_{SENSOR} = 5 \text{ ms}$).

optimal depending mainly on the reporting period (t_{REPORT}). This basically occurs when the overconsumption due to rejoin process compensates the accumulated energy consumptions of the polls. Figure 5 compares PSR between rejoining and polling strategies for single and dual architectures.

Intersection between lines with zero (points A in Figure 4) indicates the t_{REPORT} above which rejoining strategy would be more convenient for any architecture. Intersection between red and blue lines (points B in Figure 4) indicates the t_{REPORT} above which dual architecture is more efficient than single architecture.

As expected, the energy savings of rejoining strategy increases with time between reports, faster at the beginning, until reaching a final stable value. This is because increasing time between reports decreases relative impact of Q_{REJOIN} over the total. For this same reason, the final PSR is much more affected by the time between polls rather than by the value of Q_{REJOIN} .

4.3. Sleeping. As we have seen in Table 5, with any given sampling/polling/reporting conditions, the current in sleep mode is a relevant variable that has major impact in node lifetime. Thus, it is evident that the primary goal of a low power system is being in sleep mode as long as possible [35]. Some authors propose adaptive runtime to maximize efficiency [36]. Indeed, it is common to perform nodal power consumption analysis according to sleeping duty cycle [37]. Given the presented FSM tasks, considering sleeping time that is several orders of magnitude higher than the time devoted to all other tasks, having a battery charged with Q_{BATT} and “ n ” being the number of reports performed by the node during its lifetime, charge will be drained as

$$Q_{BATT} = Q_{INIT} + n \times \left(\frac{t_{REPORT}}{t_{SAMPLE}} \times Q_{SENSE} + \frac{t_{REPORT}}{t_{POLL}} \times Q_{POLL} + Q_{REPORT} + t_{REPORT} \times I_{SLEEP} \right). \quad (4)$$

Dual architecture with low power microcontrollers allows greater versatility to reduce sleep current, due to additional capabilities provided by a microcontroller: ultralow wakeup with external capacitor and radio module’s totally powered off. (Frequently, microcontrollers have external interrupts based on discharged time of a capacitor. (See Microchip AN879 Using the Microchip Ultra Low-power Wake-up Module) or high impedance RC external circuits could be used in a low power interrupt. Note that the consumption for charging this capacitor is negligible.) Both architectures can also use an external RTCC to reduce to the maximum energy required for timing. (Low-Current High-ESR Crystals (such as Maxim DS1341) with I²C communication and one output used to activate an alarm interrupt of the microcontroller.) Table 6 shows pros and cons of different sleep mode strategies, sleep current of hardware, and associated PSR of dual architecture versus single architecture.

For polling (node can receive messages) and rejoining (node cannot receive messages) configurations, we considered four sleeping strategies. Using internal or external RTCC (additional chip necessary) provides node’s conscience about clock and calendar and high precision in wakeup timing. It can be useful to build time synchronized WSNs, to accurately monitor variables or to timestamp measurements. Internal WDT reduces current consumption and loses timing functionalities. Finally, ultralow power wakeup has the most inaccurate timing (that could be enough to form any applications) but greatly reduces current consumption.

Evidently, the more the silicon modules that can be powered off, the less the power consumption in sleep mode. Thus, due to its higher flexibility, the dual architecture can be very convenient in case the application requirements allow it; it is especially remarkable to note the PSR difference in the rejoining strategy with ultralow power wakeup.

4.4. Hardware Architecture Performance Comparison. In order to range the importance of the issues described here, this section provides a hardware architecture performance comparison of well-known WSN platforms [38–40]. The methodology followed has been to model the hardware blocks of the platforms according to chip manufacturer specifications and calculate the expected battery lifetime in a realistic scenario. Table 7 show the life expectancy expressed in years and the ratio compared to the best performance architecture. (Test framework considered: $V_{supply} = 3 \text{ V}$; internal oscillator, main frequency = 8 mhz, secondary frequency = 1 MHz; External Oscillator, Crystal frequency = 32.768 kHz; $t_{SAMPLE} = 120 \text{ s}$, $t_{POLL} = 4 \text{ min}$, $t_{SENSOR} = 1 \text{ ms}$; $t_{REPORT} = 60 \text{ min}$; Battery type = LiMnO₂, model = 2032/5004LC, capacity = 210 mAh). Obviously, it is necessary to consider that older systems are at disadvantage as chipset performance improves every year.

According to the results in previous sections, dual architecture is more efficient than the single one for the given conditions. Also both Texas Instruments and Microchip-Ember provides the highest performance. As sensing duties are not exigent in terms of microcontroller requirements, we can observe the negative effect of oversizing them (SunSpot’s microcontroller is very powerful) in terms of life expectancy.

TABLE 6: PSR_{DSvsD} for several configurations ($t_{\text{SAMPLE}} = 120$ s, $t_{\text{POLL}} = 4$ min, and $t_{\text{SENSOR}} = 1$ ms).

Sleeping strategy	I_{SLEEP} (Dual)		I_{SLEEP} (Single)		PSR _{cycle} (DSvsS)	Pros and cons
	uC _{PIC} + RTCC _{DS}	RM _{Ember}	RM _{Ember}	SoC _{Ember}		
Polling	Internal RTCC wakeup	0.835 μ A	0.4 μ A	1 μ A	5.68%	+ Node can receive messages + High precision in wakeup timing
	Internal WDT wakeup	0.585 μ A	0.4 μ A	0.8 μ A	2.58%	+ Node can receive messages – Low precision in wakeup timing
	External RTCC wakeup	0.035 μ A + 0.25 μ A	0.4 μ A	0.4 μ A + 0.25 μ A	0.78%	+ Node can receive messages + High precision in wakeup timing – Additional RTCC chip necessary
	Ultralow power wakeup	0.035 μ A	0.4 μ A	0.8 μ A	–41.63%	+ Node can receive messages – The lowest precision in wakeup timing
Rejoining	Internal RTCC wakeup	0.835 μ A	0	1 μ A	–25.90%	– Node cannot receive messages + High precision in wakeup timing
	Internal WDT wakeup	0.585 μ A	0	0.8 μ A	–35.94%	– Node cannot receive messages – Low precision in wakeup timing
	External RTCC wakeup	0.035 μ A + 0.25 μ A	0	0.4 μ A + 0.25 μ A	–59.47%	– Node cannot receive messages + High precision in wakeup timing – Additional RTCC chip necessary
	Ultra low power wakeup	0.035 μ A	0	0.8 μ A	–90.66%	– Node cannot receive messages – The lowest precision in wakeup timing

TABLE 7: WSN hardware platform performance comparison.

Platform	Hardware architecture		Life expectancy (Years)	Ratio (%)	
	Microcontroller	Transceiver			
Dual	Texas Instruments	MSP43F2001	CC2530	2.75	100%
	Microchip-Ember	PIC24F16KA102	EM357	2.45	89.12%
	Iris-It (2008)	ATMega 1281	AT86RF230	1.03	37.42%
	Libelium (2012)	ATMega 1281	EM357	0.99	36.16%
	TelosB, Shimmer (2005)	MSP430F1611	CC2420	0.75	27.47%
	MicaZ (2004)	Atmega 128L	CC2420	0.42	15.11%
	Sun SPOT (2007)	AT91SAM9G20	CC2420	0.14	5.20%
Single	Texas Instruments		CC2530	2.13	74.34%
	Ember		EM357	1.42	48.90%

Also, comparing performance of platforms sharing the same transceiver (CC2420 and EM357), the influence of the microcontroller chosen is obvious.

5. Conclusions

WSNs are essential in the next generation of Internet where ubiquitous interconnected objects are available for interaction. Ubiquity means everywhere and anytime availability of sensing nodes implying wireless communication, energy harvesting, low power, and so forth; concepts that if not properly considered can lead to reduced systems' autonomy killing many real IoT applications. With these considerations in mind, low power consumption is one of the most important targets when designing IoT ready sensors.

This paper studies different sensor node hardware architectures, deepening in the power consumptions associated with each state of the runtime cycle and time-relationship

between them. It compares the energy consumption involved in the operation of a sensor node implemented using two different architectures: dual (based on a low power microcontroller and a radio module) and single (based on a system on chip). The specific finite state machine that describes the operation of sensing node is based on standard IEEE 1451 and the specific communications substates are modeled according to ZigBee Pro standard.

One important conclusion is that energy required in the sensing procedure has an important impact on this balance. There are some tasks, such as waiting for a valid sensor output (t_{SENSOR}) or acquiring the sensor data, which might require relevant amount of energy depending on the sampling rate (t_{SAMPLE}). This can turn dual architecture more efficient than the single one. One reason is that because low power microcontrollers in single architecture have higher flexibility than SoC architectures in terms of low power oscillator configurations, microcontrollers embedded in SoCs are usually

not able to run with kHz oscillators. The second reason is because low power microcontroller peripherals are more optimized, something which can be especially relevant in case of using analog sensors that require the use of analog-digital converter (the same performance in terms of quality of the conversion requires less current and time in low power microcontroller than in SoC).

Considering temporal ubiquity requirements, if the IoT application does not require nodal availability at any time (for example to change sampling parameters), nodes can disconnect from the WSN. In case of ZigBee standard, this can be implemented using rejoining and polling strategies. In that case, when energy needed to rejoin exceeds consumption due to several polls, polling strategy turns to be more energy efficient. It also shows that, above a certain reporting period, dual architecture is more efficient because rejoining strategy allows to totally power off the radio module when not using it.

Power consumption in sleep mode has major impact on node lifetime, so there is a need to design a system with a current in sleep mode as low as possible. Again, dual architecture might be more convenient because low power microcontrollers are more flexible in terms of oscillator configuration and have additional low power modules such as ultralow-power wake-up module.

The main conclusion of the study evidences that, despite what could be considered initially and stated in datasheets, no architecture is always energetically more efficient than the other; deep contextualized system analysis is mandatory to squeeze batteries to the maximum. This paper provides generic guidelines that would help electronic designers in this analysis in order to decide the most energy efficient hardware architecture of sensor nodes. We also find it useful for firmware and even software developers in order to provide understanding about how IoT application requirements (e.g., reporting time) affect WSN performance and lifetime. Finally, a performance comparison of different WSN platforms attending to their hardware architecture evidences the impact of the issues just stated.

As a final example, making clear the importance of the analysis, if a sensor that polls for data every 4 min samples every minute a sensor that needs 5 ms to set up and reports data each 4 hours is implemented using a dual architecture, it would need 24% less energy than implemented using a SoC. But just changing sampling rate from 1 minute to 5 minutes would turn the situation making the dual architecture consume 6% more energy than single architecture.

References

- [1] O. Mirabella and M. Brischetto, "A hybrid wired/wireless networking infrastructure for greenhouse management," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 2, pp. 398–407, 2011.
- [2] O. A. Postolache, P. M. B. S. Girao, J. Mendes, E. C. Pinheiro, and G. Postolache, "Physiological parameters measurement based on wheelchair embedded sensors and advanced signal processing," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 10, pp. 2564–2574, 2010.
- [3] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, 2009.
- [4] C. C. Gómez, J. Paradells, and J. E. Caballero, *Sensors Everywhere. Wireless Network Technologies and Solutions*, Fundación Vodafone España, 2010.
- [5] A. Sharma, K. Shinghal, R. Singh, and N. Srivastaya, "Energy management for wireless sensor network nodes," *International Journal of Advances in Engineering & Technology*, vol. 1, pp. 7–13, 2011.
- [6] C. Knight, J. Davidson, and S. Behrens, "Energy options for wireless sensor nodes," *Sensors*, vol. 8, no. 12, pp. 8037–8066, 2008.
- [7] R. Soua and P. Mine, "A survey on energy efficient techniques in wireless sensor networks," in *Proceedings of the Wireless and Mobile Networking Conference (WMNC '11)*, INRIA, Le Chesnay, France, 2011.
- [8] J. E. Higuera and J. Polo, "IEEE 1451 standard in 6LoWPAN sensor networks using a compact physical-layer transducer electronic datasheet," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 8, pp. 2751–2758, 2011.
- [9] IEEE Standard 1451.5, "IEEE standard for a smart transducer interface for sensors and actuators—wireless communication protocols and transducer electronic data sheet (TEDS) formats," IEEE, 2007.
- [10] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.
- [11] ZigBee Alliance, "ZigBee Specification," Document 053474r17, 2008.
- [12] R. X. Gao and Z. Fan, "Architectural design of a sensory node controller for optimized energy utilization in sensor networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 55, no. 2, pp. 415–428, 2006.
- [13] S. Bilouhan and R. Gupta, "Optimization of power consumption in wireless sensor networks," *International Journal of Scientific & Engineering Research*, vol. 2, no. 5, 2011.
- [14] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, 2005.
- [15] M. Al Ameen, S. M. R. Islam, and K. Kwak, "Energy saving mechanisms for MAC protocols in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2010, Article ID 163413, 16 pages, 2010.
- [16] S. M. Ahmad Madani, *Cross layer design for low power wireless sensor networks [Ph.D. thesis]*, 2008.
- [17] P. Yu, L. Qinghua, and P. Xiyuan, "The design of low-power wireless sensor node," in *Proceedings of the IEEE International Instrumentation and Measurement Technology Conference (I2MTC '10)*, pp. 917–922, May 2010.
- [18] T. R. Park and M. J. Lee, "Power saving algorithms for wireless sensor networks on IEEE 802.15.4," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 148–155, 2008.
- [19] F. Salvadori, M. de Campos, P. S. Sausen et al., "Monitoring in industrial systems using wireless sensor network with dynamic power management," *IEEE Transactions on Instrumentation and Measurement*, vol. 58, no. 9, pp. 3104–3111, 2009.
- [20] S. Caban, G. José Antonio, and M. Rupp, "Measuring the physical layer performance of wireless communication systems," *IEEE Instrumentation & Measurement Magazine*, vol. 14, no. 5, pp. 8–17, 2011.

- [21] C. Alippi, G. Anastasi, M. Di Francesco, and M. Roveri, "Energy management in wireless sensor networks with energy-hungry sensors," *IEEE Instrumentation and Measurement Magazine*, vol. 12, no. 2, pp. 16–23, 2009.
- [22] Texas Instruments Incorporated, <http://www.ti.com/product/cc2420>.
- [23] "XP Semiconductors N.V.," <http://www.nxp.com/campaigns/i2c-bus/>.
- [24] "Silicon Laboratories Inc.," <http://www.silabs.com/products/wireless/zigbee/Pages/zigbee-chips-em35x.aspx>.
- [25] "Texas Instruments Incorporated," <http://www.ti.com/product/cc2530>.
- [26] P. H. Chou and C. Park, "Energy-efficient platform designs for real-world wireless sensing applications," in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD '05)*, pp. 913–920, November 2005.
- [27] M. Gao, X. Pan, L. Deng, C. Huang, D. Zhang, and L. Ni, "A versatile nodal energy consumption monitoring method for wireless sensor networks testbed," in *Proceedings of the IEEE 17th International Conference on Parallel and Distributed Systems*, pp. 388–395, 2011.
- [28] Castalia, <http://castalia.research.nicta.com.au/index.php/en/>.
- [29] G. V. Merrett, N. M. White, N. R. Harris, and B. M. Al-Hashimi, "Energy-aware simulation for wireless sensor networks," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09)*, June 2009.
- [30] P. Yu, L. Qinghua, and P. Xiyuan, "The design of low-power wireless sensor node," in *Proceedings of the IEEE International Instrumentation and Measurement Technology Conference (I2MTC '10)*, pp. 917–922, May 2010.
- [31] H.-Y. Zhou, D.-Y. Luo, Y. Gao, and D.-C. Zuo, "Modeling of node energy consumption for wireless sensor networks," *Wireless Sensor Networks*, vol. 3, no. 1, pp. 18–23, 2011.
- [32] E. Casilari, J. M. Cano-García, and G. Campos-Garrido, "Modeling of current consumption in 802.15.4/ZigBee sensor motes," *Sensors*, vol. 10, no. 6, pp. 5443–5468, 2010.
- [33] B. Gholamzadeh and H. Nabovati, "Concepts for designing low power wireless sensor network," *World Academy of Science, Engineering and Technology*, vol. 45, pp. 559–565, 2008.
- [34] W. S. Wang, R. O'Keeffe, N. Wang, M. Hayes, B. O. Flynn, and S. C. Ó Mathúna, "Reducing power consumption in metrics for building energy management applications," in *Proceedings of the 23rd European Conference Forum Bauinformatik*, Cork, Ireland, 2011.
- [35] A. Viswanathan and T. E. Boulton, "Power conservation in ZigBee networks using temporal control," in *Proceedings of the 2nd International Symposium on Wireless Pervasive Computing*, pp. 175–180, University of Colorado Press, Boulder, Colo, USA, February 2007.
- [36] J. Chern Lim and C. Bleakley, "Adaptive WSN scheduling for lifetime extension in environmental monitoring applications," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 286981, 17 pages, 2012.
- [37] Y. W. Chung and H. Y. Hwang, "Modeling and analysis of energy conservation scheme based on duty cycling in wireless Ad Hoc sensor network," *Sensors*, vol. 10, no. 6, pp. 5569–5589, 2010.
- [38] V. Madan and S. Reddy, "Review of wireless sensor mote platforms," *VSRD International Journal of Electrical, Electronics & Communication Engineering*, vol. 2, no. 2, pp. 50–55, 2012.
- [39] T. V. Chien, H. Nguyen Chan, and T. Nguyen Huu, "A comparative study on hardware platforms for wireless sensor networks," *International Journal on Advanced Science Engineering Information Technology*, vol. 2, no. 1, 2012.
- [40] R. Lajara, J. Pelegrí-Sebastiá, and J. J. Perez Solano, "Power consumption analysis of operating systems for wireless sensor networks," *Sensors*, vol. 10, no. 6, pp. 5809–5826, 2010.

2.2 ENERGY-AWARENESS APPLICATION FOR THE INTERNET OF THINGS



Asensio Gimeno, Ángel; Marco Marco, Álvaro; Blasco Marín, Rubén; Nebra Casas, Roberto; Bascuas Blanco, Teresa; Trasviña-Moreno Carlos.
Journal of Sensor Networks (ENVIADO)

2015

RESUMEN:

Este trabajo recoge los resultados de dos implementaciones reales de sistemas IoT. El objetivo en ambos casos era disponer de un sistema que fuese capaz de analizar el gasto energético de una edificación y aconsejar a sus usuarios patrones de hábitos para reducirlo. Estos sistemas tienen como base una arquitectura WSN, en la que es crítico que sus nodos sean eficientes (no es viable la sustitución periódica de sus baterías), pero además se requieren otras capacidades a las que IoT puede dar respuesta. De este modo, el desarrollo de la primera implementación coincidió cronológicamente con la investigación asociada al manuscrito anterior.

En el primer ejemplo, en el marco del proyecto Reinassance se desplegó un sistema en 35 domicilios particulares. Al abordar este proyecto surgieron una serie de retos en cuanto a la arquitectura de sistema, y la interoperabilidad entre dispositivos. La investigación y resultados al respecto motivaron el “Manuscrito 3 (Interoperabilidad)”. Una vez desplegado el sistema permaneció operativo durante 6 meses. Finalizada esta fase tras el buen desempeño del sistema y los avances conseguidos (que serán referidos en “Manuscrito 3”) se optó por evolucionar el sistema para aplicarlo al proyecto Liga Energética que supuso el despliegue de cerca de 200 nodos en el Edificio de los Institutos de la Universidad de Zaragoza, en el que permaneció activo durante otras 24 semanas. (Nótese que los largos periodos de puesta en servicio explican porque este manuscrito es cronológicamente posterior al resto pese a que los trabajos desarrollados en el mismo sean previos).

Energy-Awareness application for the Internet of Things

Ángel Asensio¹, Rubén Blasco¹, Álvaro Marco¹, Roberto Casas¹, Teresa Blanco¹, Carlos Trasviña-Moreno¹

¹ Aragon Institute of Research, Universidad Zaragoza {aasensio, rblasco, amarco, teresa.blanco, rcasas, ctrasvina}@humanopenware.com

Residential energy consumption represents an important ratio of the total energy consumed in the world. User awareness and best practices education to have an energetically responsible behaviour has a great impact on efficiency. This paper presents a novel Internet of Things (IoT) system that provides context-based feedback to the user of a household or building about their habits regarding energy use and suggestions in order to improve them. Services provided by the Energy Aware system shown in this paper are based in a Network of Things (NoT) including sensors to perceive context, actuators and tangible interfaces to provide natural interaction. It guarantees interoperability with other sensor networks, fast service development, easy deployment, maintenance and update thanks to its OSGi-based middleware.

Keywords: Energy-awareness; Internet of Things, Wireless Sensor Network, OSGi

1 Introduction

The increased levels of CO₂ concentration and other greenhouse gases in the atmosphere due to human activity are leading to a rise in the temperature of the planet. From the grand total, household energy consumption (Pérez-Lombard, Ortiz & Pout 2008) currently represents 26% of total EU (Eurostat-European Commission 2011) and 23% in the U.S. (U.S. Energy Information Administration 2015). Based on current projections, global temperature is expected to increase between 0.1° and 0.2° by decade, causing significant changes in the climate (Pachauri et al. 2014). There is strong evidence that informing and educating people, in order to improve their energy habits, is a very effective immediate action (Froehlich 2009), (Miroso, Lawson & Gnoth 2013), (Barbato et al. 2009).

In this paper we show the design and development of an energy and ambient monitoring kit that could be easily installed into dwellings or buildings. The kit allows the neighbors (or building manager) to know their energy consumption (electricity, heating) as well as the temperature and humidity in different parts of the building. In addition, this information is sent to the *cloud* to be analyzed remotely in order to suggest changes that could allow users to cut back their energy consumption.

Traditionally these projects are solved by using WSN (Wireless Sensor Networks) (Erol-Kantarci, Mouftah 2011), (Dong et al. 2010) however in this case, there are

some additional requirements that with a classical architecture would not be solved optimally:

- Heterogeneity of included devices, both for its use (sensors, actuators and HMI) and for different manufacturers.
- Need of remote access to the system for collecting information to generate real-time recommendations.
- Capability to interact with every other device.
- The installation, maintenance and use should be simple.
- The system should be able to be used in different scenarios.

Therefore it was decided to develop an Internet of Things (IoT) solution, evolving the existing proposals based on WSN. The IoT concept proposes that everyday objects are globally accessible from the Internet and integrate into new services having a remarkable impact in our society. A *Thing* could be any device that is around us (Gubbi et al. 2013). In this project we use *Things* especially designed to be aware of ambient and energy and share this information through Internet.

The proposed solution has been evaluated in two deployments with different requirements but with the same purpose: improving energy efficiency through user awareness. The system was initially developed to be used as the technological infrastructure of a living-lab within the European project *Renaissance* (Renaissance 2015) (research and demonstration project of the CONCERTO initiative (European Union initiative 2015) funded by the European Commission through the 6th Framework Programme). During this

project, 35 houses used the system successfully for 6 months. Later the same systems were reconditioned for use in Energetic League project (HOWLab-GEE 2015), that deployed near two hundreds *Things* into I+D+i building of the University of Zaragoza for 24 weeks.

Similar deployments already exist (Sundramoorthy et al. 2010), (Schwartz et al. 2014) and information recollected has been of great interest. Even though the data extracted from these projects is invaluable for this proposal, the main purpose of this paper is to present the technological infrastructure and not the interpretation of the information or results.

This paper describes an IoT based on a developed WSN energy aware Kit, and is organized as follows: section two discusses the related work in the field; sections three and four describe the system components and its architecture; and section five summarize the deployment done in the *Renaissance* and Energetic League projects. and final section concludes the paper.

2 Related work

Ambient intelligence (Aml) has an important impact in multiple fields enabling energy savings and emissions reduction (Paola et al. 2015). In order to create such smart spaces, several aspects must be taken into consideration: ubiquitous computing, natural interaction, context awareness, emotional computing, artificial intelligence, etc. (Ramos, Augusto & Shapiro 2008). Currently, thanks to the low cost sensing technologies, the increment of processing capacity and evolution of wireless communications, it is possible to achieve a real ubiquitous and distributed computation (Kulkarni, Förster & Venayagamoorthy 2011). This enables intelligent systems to increasingly have more contextual information to help in the decision-making. According to EC (European Commission), the next decade will be dedicated to the Future Internet with the IoT (ISTAG 2015) as its maximum exponent. Distributed wireless sensor networks are a key piece in this puzzle, as they are mainly responsible of providing context awareness (Robinson, Sanders & Mazharsolook 2014). The establishment of IoT requires one step further in this direction: smart infrastructures of embedded devices with local intelligence and access to the “information word”, Internet, and interaction with each other’s.

Energy usage in buildings is high, consequently it represent an important part of the total amount of energy related to the operation of a city. Thus an energy-aware system could be interesting for the development of both Smart City and Smart Grid (Gungor, Lu & Hancke 2010). Using de paradigm of IoT is possible join together all these proposals (Moreno et

al. 2014). IoT is also a mechanism used to get in touch with the social networks using real *Things* around us. This is interesting due to the ability of social networks to possibly raise awareness of energy consumption (Ciuciu, Meersman & Dillon 2012).

Focusing on households or buildings for the development of an energy-awareness IoT system that helps and guides users, the first step is to monitor some parameters. The most relevant are: electricity, hot sanitary water, heating system (electricity, gas or other) and cooling system (electricity) as they contribute to the majority of energy usage. Furthermore, additional parameters such as temperature, humidity, light intensity and presence are essential when sensing comfort and characterizing user habits of energy expenditure and its relation with the building consumption.

There are different approaches addressing this problem as a complete system (Marinakakis et al. 2013). Logically, these usually make use of paradigms related with Smart Home (Han, Lim 2010). For example the most widely used communication protocols in energy awareness systems are ZigBee, PLC (Power Line Communication), WiFi and infrared (Han et al. 2014).

All these systems are based on some type of energy measurement (Kim, Lee & Hwang 2011). In some cases the system itself is capable of acting for adjust the energetic consumption. This is usually done by controlling the demand for electricity (Byun, Park 2011). This can be achieved in several manners, for example (Han, Choi & Lee 2011) proposes a system based on ZigBee and an infrared remote controller that reduces the standby power consumption of the appliance. Other solutions propose an individual control on each one of the electric charges (Kuzlu, Pipattanasomporn & Rahman 2012). The proposals of the latter type are closely related to the concept of Smart Grid (Aman, Simmhan & Prasanna 2013).

With the previous system examples, specific devices can be found, primarily aimed at end users. Within these two exemplifications include:

- Smart thermostats, as proposed by (Lu et al. 2010) that incorporated occupancy sensors or the Nest Learning Thermostat (Nest 2015) (developed by Nest, a startup acquired by Google that today is one of the most dynamic actors of IoT).
- Power monitors for an easy electricity consumption management, among which there are multiple alternatives according to their characteristics (power, communications, logger, etc.) (Alahmad et al. 2012). The growing concern of users to reduce their energy consumption, drives the market to create commercial plug-and-play devices (Saveometer 2015), (Efergy 2015).

Despite these examples, there are two important barriers regarding the complexity associated to the management and deployment of such systems. The

first is that it is necessary that the deployment of the system be simple and fast, which means that *Thing* should preferably be wireless and with no maintenance. Therefore *Things* should have a high operating autonomy. In the area of WSN, numerous research has been done regarding the design of low power nodes which are applicable to the design of *Things* as this project requires.

The second barrier is the poor interaction amongst devices, derived from a large number of these, present in real IoT scenarios, and their heterogeneous origin. It is fairly common to find that various manufacturers use different technologies and protocols, thus creating an incompatible network environment. As a solution to guarantee this required interoperability, middleware architectures have become a key research topic.

Within this subject, the Service-Oriented Architectures (SOA) have proven to be an efficient tool to develop applications based on interoperable services. Specifically, the usage of the Open Services Gateway Initiative framework (OSGi) (OSGi Alliance 2015), in systems supporting the deployment of an IoT, facilitates the development of modular software, easily scalable and upgradeable remotely.

OSGi framework offers a service platform for Java programming language where the pieces of code are organized in bundles, which can then be managed dynamically. This is one of the key strengths of OSGi, allowing updating, stopping or starting bundles dynamically without stopping the full application. Within the framework, each bundle serves to a specific task, publishing services that can be retrieved and used by other bundles, which cooperate to carry out the main application behaviour.

This framework, which was initially developed for home automation use, has proven particularly useful for the development of Aml or IoT systems, as it allows the independence between the physical nature of the Smart Thing on the environment and their control logic. In fact, it is broadly used in applications which need a deployment of wireless sensor and actuator networks (Ha 2009), (Lai et al. 2011), (Cheng, Wang & Horng 2012), (Paganelli et al. 2015), (Arnold, Sankur & Auslander 2013), (Chen, Wu 2012).

3 System description

The objective of the proposed solution is to acquire user patterns, relating to their energy consumption and comfort variables, and then issue recommendations in order to increase their awareness and enhance energy savings. This requires an accurate monitoring of energy consumption and environmental conditions over a long period of time, in order to generate enough data to extract relevant information. To accomplish this goal,

the system depicted in Figure 1 has been used, which comprises three major blocks: **Networks of Things, gateway and IoT and Local Services.**

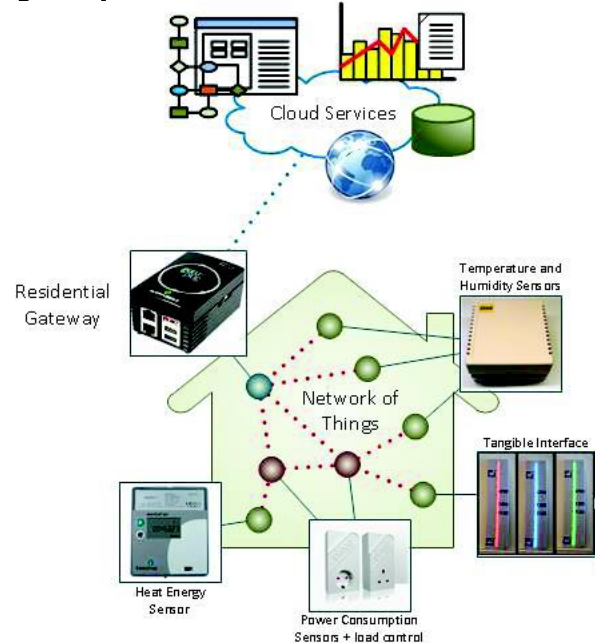


Figure 1. WSN monitoring system architecture. (Renaissance Project use case)

The *Things* world can be defined as where micro-electromechanical systems, smart sensors, simple human-machine interfaces (HMIs), etc. associate in networks (Networks of Things, NoT) to ubiquitously interact with other *Things*, environment and people. The Internet world usually is constructed around computers, centralized software infrastructures or in the *cloud* [16]. Applications and services use *Things* to provide context awareness, artificial intelligence, affective computing, etc. [16]. Internet acts as the base infrastructure for the exchange of information. However, to join together all these aspects it is necessary to overcome several requirements such as the need for a unique identifier, changing the communication technology and the adoption of the Internet Protocols. Nowadays, this "IP wall" is usually jumped through an IoT gateway.

3.1 Network of Things (NoT)

For the current proposal, a NoT has been developed with the objective of monitoring environmental conditions (temperature and humidity) and the electric power consumption (whole house and in some cases the contribution of air conditioning), without modifying the current infrastructure (electrical and heating).

To capture this information different *Things* (acting as Smart Sensors) have been developed. These represent part of a family of devices developed on the framework of OpenLab and the Zeta Project (HOWLab 2015). Zeta Project includes different sensors,

actuators and user interaction devices (named *Zmotas*), specifically designed for an ultralow power consumption. They are based on an 8 bit microcontroller and include ZigBee Pro standard communication.

Amongst these *Zmotas*, the *ZmotaAMBI* device was designed to capture temperature and humidity data in a low power consumption mode. This allows several years of battery life, while monitoring every 10 minutes and configured as Reduced Function Device (RFD). It also integrates an expansion port which allows the management of smart sensors or meters through a serial interface (UART, I2C or SPI). Specifically this port is used to communicate with a commercial heat meter, namely the Multical 402 from Kamstrup (Kamstrup 2015), which measures the heat energy consumption of the household.

We also developed *ZpetaPEM*, an energy monitor device that can measure RMS voltage, current and Power. Nonetheless to avoid normative procedures, (when the system is used in real scenarios) and prove system interoperability, we decided to use a commercial meter from Efergy (Efergy 2015) (connecting its engage hub to our gateway) in households (Renaissance project). As the *Liga Energética* project was deployed in buildings in which we are located, we assume that we can install both devices. At the same time we used the commercial system to validate the measurements of our device.

To bridge the gap between the information perceived by the sensors and monitors with the user, tangible interfaces are used. These are simple and pervasive devices that enable interaction with other artefacts and with people with great ease. They are useful for natural user awareness on energy consumption (e.g. a device glowing red when above the average consumption) or advising on efficiency strategies (Karlgrén et al. 2008). Thus, with this idea in mind, the *ZmotaZEN* was developed. This device is able to play music/talk/make sounds and illuminate with up to 40 independent RGB LEDs. This device can be encapsulated in different form factors: a glowing ball, a row of lights, etc.

All these devices send data through the network coordinator, *ZlitaUSB*, which could also behave as a sink. In this case, the device is connected to a USB port in the gateway, communicating with an AT command interface. This same device can be equipped with an external antenna, connect to the grid and act as a router of the ZigBee network.

3.2 Gateway

The next element of the system is the Gateway which is in charge of creating and maintaining our ZigBee NoT, as well as other networks, *Thing* recognition and the collection of the data generated by the *Things*. In addition to connectivity with the NoT through the

ZlitaUSB, the Gateway is also connected to the Internet, granting access to *cloud* services. According to the usage scenario there are different devices that can act as a Gateway.

In the *Renaissance* project we have chosen a commercial embedded PC from Globalscale Technologies (Globalscale Technologies 2015), namely the GuruPlug. It fulfils our functional requirements and shows added value characteristics such as a small form factor, a direct connection into a wall outlet and an ultralow power consumption (under 5 watts). We installed a Java Virtual Machine, and chose the OSGi framework Karaf (Karaf 2015), which provides additional features such as logging subsystem and remote console access, to deploy the monitoring system services. It is a perfect solution for use in a household, because it requires minimal and non-invasive setup, only plugging into a wall outlet and the connection to a WiFi router.

The gateway of course could be an “always on” PC that has internet connection. This is the typical choice in case of applying the system to an entire building, since it probably already has a PC or similar in charge of the management of other systems (heating, lighting, etc.). Hence, this is the selected for *Liga Energética* project where the deployment is more complex (more and different *Things*), and the same PC can be used for database management and *cloud* services deployment.

For the current implementation, we are using a BeagleBone Black (BeagleBoard.org 2015), an intermediate solution that could be useful in other scenarios such as remote areas (with its corresponding power source), industrial environment, cost sensitive application, etc. Using this kind of Open Hardware SBC (Single Board Computer) has the advantage of allowing the incorporation of additional modules (named Beagle-capes) over the SBC itself, adding extra functionality (such as new wireless communications technologies).

3.3 IoT and Local Services

Information gathered by the NoT is processed by IoT services (that are in the *cloud*) in order to derive user habits on power consumption and issue the recommendations for efficient usage of the energy. The addressee of this information may be either an individual user who lives in the household as the manager of a building. Depending on the addressee, complexity and detail of the information processed varies. Although data processing could be carried out locally, whether on the residential gateway or even in the smart devices, moving them to the *cloud* provides several advantages.

Making sensing data available to a central server allows aggregation of the data from several consumers allowing identification of patterns and establishment of

correlations among users to derive global consumption habits, user profiling according to common behaviours, geographical location or climatic constraints. Besides visualizing user's own energy consumption data, the *cloud* approach allows users comparing their figures with those of users with similar profiles, detecting abnormal situations like unexpected energy consumption deviations which may suggest wrong conditioning or use of the house.

Hosting services in the *cloud* also simplifies deployment of new services, as they do not need to be distributed on every installation, only in the main application host. Furthermore, the software architecture on the gateway minimizes the effort required for remote provisioning of local services.

This also opens possibilities for remote or local definition of new services to operate, whether at the residential gateway or at the smart devices network. A simple, yet effective, application of this could be issuing a red colour command in the tangible interface when the temperature rises above a predefined threshold at the sensor and the heat sensor is registering instant heat consumption.

The aim of the developed solution is to reduce energy consumption informing and forming the user to be a wise consumer that has the freedom to decide instead of with an active and automatic control of the consumption. However, the system architecture also allows services for proactively acting over the energy consumption. Operating automatically over household devices is convenient in several situations such as when the user is not present at home, not able to control (e.g. because he/she has a disability) or not aware of specific situations that require actuation over loads (e.g. forget about turning the heating on when leaving the house). This is easily possible by incorporating *Things* with control capacity, such as other of our *Zmota* devices: one acting as a relay board for on/off load switching and another is a device with SSR (Solid State Relay) control that enables a modulation over the load.

4 System Architecture

From a technological perspective, there are different ways of implementing IoT systems depending on where the intelligence that provides the perceived services resides. It can be totally distributed over the smart devices, centralized in specific smarter computers or servers, distributed in the *cloud*, etc. Each approach poses pros and cons such as ease of deployment, maintenance, configuration, cost, energy supply, etc. Whichever the case, we can distinguish two well differenced worlds with diverse characteristics (Atzori, Iera & Morabito 2010):

- Lower layer, where micro-electromechanical systems, wireless smart device networks,

embedded systems, etc. are distributed across the real world to ubiquitously interact with it.

- Higher layer, that usually runs furthest from the real world in centralized software infrastructures or in the *cloud*, through global communication—usually IP—, where apps and/or services provide artificial intelligence, affective computing, data management, etc.

According to the state of the art, most systems follow the archetypes just described, where one or more networks interact with environment and people. The devices in these networks exchange information with the IP-world through gateways, DTNs (Delay and Disruption-tolerant Interoperable Networking), SCADAs (Supervisory Control and Data Acquisition) (Grilo et al. 2014), directly connecting to the Internet, etc. (Rodrigues, Neves 2010), (Zhengguo Sheng et al. 2013). Inherent to this, two challenges arise: interoperability between the two worlds and development of services and applications.

4.1 NoT Architecture

NoT architecture must ensure interoperability between devices in the same network, this is one of the major challenges for the IoT. There are different approaches aiming for the same objective: communication standards such as ZigBee or 6LoWPAN and protocol-independent proposals such as IEEE1451. IEEE1451 describes a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field network (Song, Lee 2008). Thus, theoretically it is the best suited option as it provides independence from the communication protocol. Nevertheless, its penetration in real applications is very limited, with little hardware available and mainly relegating it to the electronic instrumentation field.

In the scenario where a new single NoT is required, ZigBee seems to be the most viable communication protocol, as it is commonly used in IoT applications. Besides interoperability at lower communication levels (network management and maintenance, security, data exchange, etc.) it defines how the devices must exchange application data attending to defined clusters (Specification 2008). For example, every ZigBee Pro compliant temperature sensor must implement “measurement & sensing cluster” and any other device in the network would be able to get temperature information as defined in the specification. Additionally, the standard defines how to create virtual bindings among devices. This allows to instantiate some intelligence in the network, programming automatic triggers from other nodes.

However selecting a particular standard (as ZigBee) involve hardware restrictions with other protocols (WiFi, Bluetooth) and lack of interoperability among

not certified devices in that standard (ZigBee-Pro Certified). To address this issue, we use Common Things Protocol (CTP) (Asensio et al. 2014) over ZigBee as a mechanism to achieve interoperability between *Things*. The CTP is a proposal of protocol oriented to interoperability that we have been developing in recent years. It aims to provide a specification that allows interoperability among communication standards and coexistence with IoT protocols, but prioritizing simplicity, efficiency and functionality to build final IoT systems. CTP takes into consideration existing specifications in the standards and the needs from the final applications that are to be supported by the *Things* in the field. It integrates the strategies, concepts and terms of some of the alternatives; for example IEEE1451 TED's concept to provide device's information, sensor and actuator working modes, etc. or ZigBee concepts of clusters and endpoints. CTP definition is approached from an ontological perspective considering *Thing* as electronic devices that perform different function in the IoT.

Implementation of the smart devices (Figure 2) follows a dual hardware architecture where a low power microcontroller (PIC18F26J11) runs the application and controls a network co-processor implementing ZigBee Pro stack (Ember 357). After deep analysis and experimentation, we found this architecture more efficient in terms of power consumption than using a system on chip solution (embedding a radio module plus a programmable microcontroller) as it allows splitting tasks between two specialized microcontrollers; one for sensing tasks and second for communication (Asensio et al. 2013).

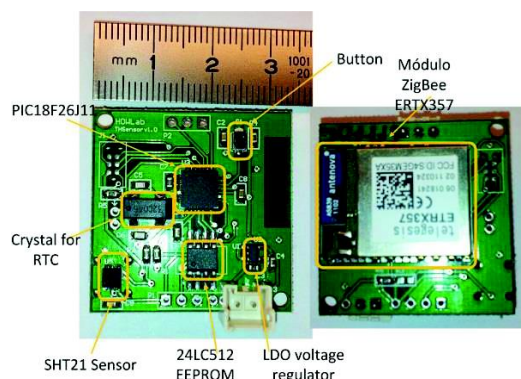


Figure 2. Zmota AMBI

4.2 Middleware Architecture

Middleware is the bridge between WSDN (Web Services Development Network) and the *cloud* regardless the WSDN technology used. Using OSGi as development framework eases development of these layers, as we may focus on one single layer when developing, while the whole application layers will be arranged on execution time. Each layer may comprise of one or more *bundles* (isolated fragments of code that

implement some behaviour and are accessible to other bundles by publishing services in the OSGi framework.)

Middle-layer interfaces are defined to specify interoperability among adjacent layers and eliminate direct dependencies among bundles implementing each layer. They specify which services and objects may be used in transactions between adjacent upper and lower layers.

Figure 3 shows the proposed architecture where we can identify several layers:

1. Serial Communication Layer (SCL).
2. Zigbee Layer (ZL).
 - 2.1. Zigbee Gateway Sub-Layer (ZGSL).
 - 2.2. Zigbee Driver Sub-Layer (ZDSL).
3. OSGi4AMI Devices Layer (O4ADL)

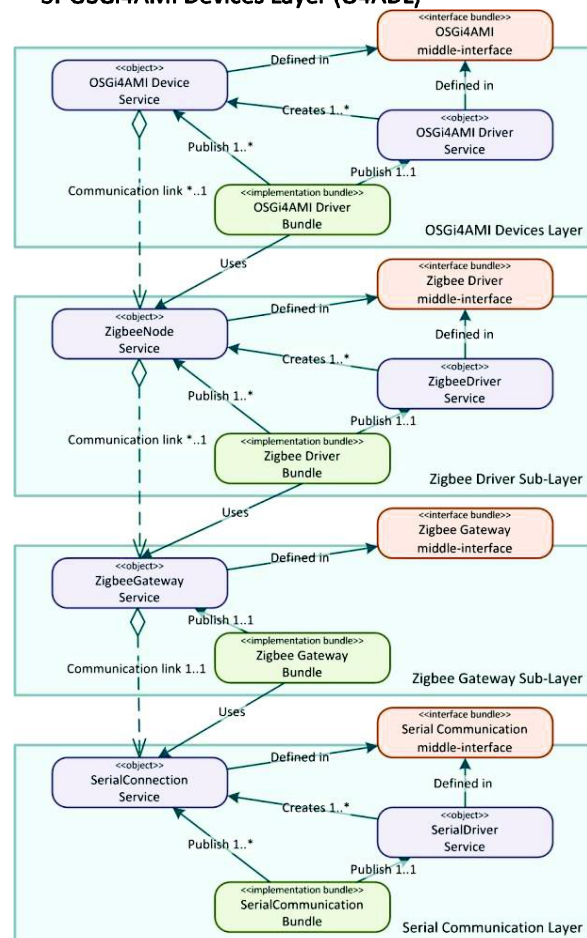


Figure 3. System middleware architecture.

Serial Communication Layer provides raw access to the serial port which allows communication with the ZlitaUSB. The serial middle-interface defines a SerialConnection service, which basically allows writing bytes and notifies about incoming bytes, and a SerialDriver service, which is in charge of creating and discovering available SerialConnections. The main bundle implementing SCL operates the UART interface, but other stream-based interfaces, such as a Bluetooth connection, may adopt the same middle-layer interface, allowing communication with Bluetooth

devices transparently to the upper layers. In our particular case, we have implemented an application service that wraps a `SerialConnection` into a TCP socket, and at the remote client, another bundle creates a `SerialConnection` that allows communication with the `SerialConnection` on the server side like a local one.

The Zigbee Layer is comprised by two sub-layers: Zigbee Gateway Sub-Layer and Zigbee Driver Sub-Layer. This is because there are several versions of the communication API with the *ZlitaUSB*, which lead us to split the layer to ease development. Zigbee Gateway Sub-Layer encapsulates the communication with the *ZlitaUSB*, implementing its communication protocol by means of a ZigbeeGateway service. When a `SerialConnection` is published by the SCL, the ZGSL bundle checks whether it corresponds to a *ZlitaUSB*, and it publishes a ZigbeeGateway in such a case. Above it, the Zigbee Driver Sub-Layer creates a ZigbeeDriver service that uses the ZigbeeGateway to accomplish network operations, such as network creation, devices discovering or error maintenance. For every node discovered on the network, the ZigbeeDriver creates and publishes a ZigbeeNode service representing that device, which allows sending and receiving messages to and from the physical device, and provides ZigBee related properties such as its MAC address or its type.

On the upper layer of the architecture the *OSGi4AMI devices layer* can be found. OSGi4AMI states for ontology which model devices can be available on Ambient Intelligence environments (Marco et al. 2009). The OSGi4AMI middle-interface provides generic interfaces for common sensors, actuators and tangible interfaces. For example, we could be defined a TemperatureSensor or OutletActuator, which allow reading temperature or actuate over mains powered devices, respectively. The OSGi4AMI driver bundle publishes an OSGi4AMI Driver service that tracks for ZigbeeNode services, discover the functionalities that physical devices provide (temperature sensing, humidity sensing, etc.), and creates OSGi4AMI Devices services which encapsulate those functionalities. The *ZMotaAMBI* presented in section 3 is able to measure temperature and humidity, and communicate with a commercial heat meter. When the driver discovers those functionalities in a ZigbeeNode, in accordance with OSGi4AMI ontology, it will create a TemperatureSensor, a HumiditySensor and a HeatMeterSensor for each ZigbeeNode associated with a *ZMotaAMBI* sensor, having a communication link with the ZigbeeNode. The commercial Plogg sensor measures power consumption and it is able to turn on-off mains powered devices. The same with the *ZMotaAMBI*, when the driver discovers those functionalities in the ZigbeeNode, it will publish a PowerSensor and an OutletActuator as defined by OSGi4AMI.

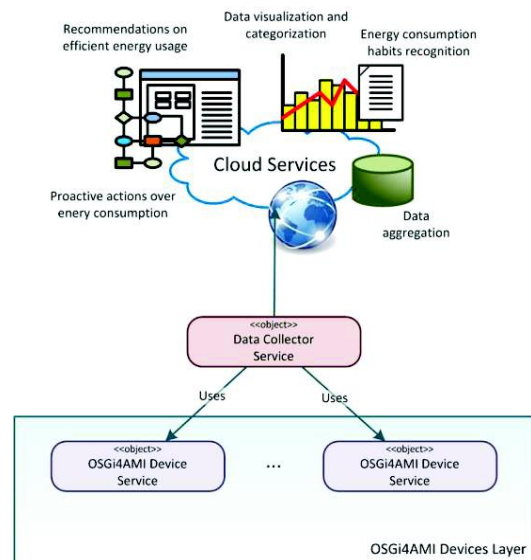


Figure 4. Data collector service.

At the top of the architecture, the *Data Collector* service, depicted in Figure 4, keeps track of OSGi4AMI devices published in the framework and checks if they are listed in the service configuration, establishing their data refresh rate and subscribing for data updates on them. When any device notifies about new data received, the collector service retrieve the sensing data, timestamp, location, etc. and upload it to the *cloud* where it is registered. The service also notifies about missing sensors and others events such as low battery or connection errors by sending e-mails to a support account.

IoT services access that central data server to accomplish data aggregation, energy consumption habits identification and derive recommendations on efficient energy usage. Users may access these services and visualize their data, comparing categorized profiles or users with similar constraints.

5 Living-lab deployment

The living-lab for Renaissance is a community in Valdespartera neighborhood (Zaragoza, Spain) which so far comprises 35 households (and is expected to reach hundreds). Each dwelling has a monitoring system running, reporting data regarding the energy habits of its inhabitants and receiving advices. These houses are distributed in different geographical areas as shown in Figure 5. This allows for a correlation among consumption habits of users in similar areas, and evidences differences when dwellings facing south or north.

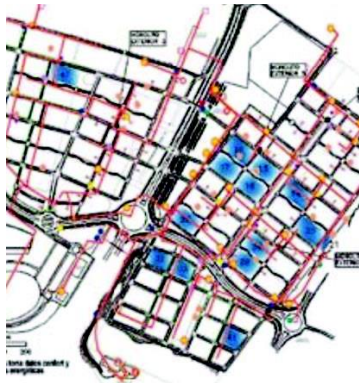


Figure 5. Living-lab community in Valdespartera neighborhood (Zaragoza, Spain).

In order to simplify the deployment of the system and minimize the installation time in the user houses, an Installation Software Tool using the same middleware architecture than the Data Collector, described in previous section, was developed. The application establishes connection with two *ZlitaUSB*: one on the residential gateway (which creates the WSDN in the home) and one in the installer's laptop (which creates a default configuration ZigBee network). It allows listing nodes on the configuration network and verifying successful deployment on the working network created by the *ZlitaUSB* connected to the residential gateway. This step is required as the ZigBee working network must be created in place for optimal channel selection, so nodes cannot be factory pre-configured. After deploying nodes to the working network, the installer generates the configuration for the data collector service, including the list of sensors deployed, their location and additional configuration parameters of the service. To the current date, the system has been running for six months without interrupting the service, not needing battery replacement and receiving remote software updates.

The robustness and reliability shown by the system on the living-lab and the lab installation, invites to extending the trials to other deployments. This is the case of the *Liga Energética* project in which the objective was to monitor the building I+D+i of the University of Zaragoza, located on the Mariano Esquillor Street. This building has an area of 14000 square meters, divided into 8 blocks of three floors connected by a central courtyard. When installing the system, the requirements are different from those of the Renaissance project, where the installation needed to be done as quickly as possible, while in this case there was no time restriction. The main difference is that in this scenario the area to cover is higher, which could produce some radio coverage problems. Therefore, in the Installation Software Tool was included a new tool that allowed network quality analysis, based on routines of sending and receiving message packets and its RSSI and LQI analysis. Using a

laptop with a *ZLita* connected and moving along all the building, we could map the building to determine the best location for the router.

6 Conclusions

This paper presents an energy and ambient monitoring system, based on an IoT architecture. It is developed to provide feedback to the household inhabitants, manager or users of a building about their habits, patterns in the use of the energy, and to provide suggestions in order to improve them. It has been shown that the WSNs incorporated into the paradigm of IoT are very powerful solutions for developing energy awareness systems. The proposed solution is able to integrate our ad-hoc WSN with devices from other manufacturers that are already installed on-site.

So far, the concept was validated in the frame of two projects: *Renaissance* project and *Liga Energética*. In the first case, the system was applied to 35 reduced areas (households) with a few *Things* in each of them, whereas in the second case was in a single wide space (an entire building) that included almost two hundred *Things*. The possibility of applying the proposal on different scenarios indicates that the solution is versatile and useful.

Technologically it is based in a wireless sensor network and in OSGi as middleware technology that together constitute a system for IoT. This system is developed under open hardware and software principles providing a robust tool which is available to be used by the community; the Zeta project. Thus, it can be said that the outcome of the project could be considered as an IoT kit for energy-awareness for both home users without much technical knowledge, and for building managers who need a more complex system. For use inside NoT, have been proposed CTP (the full specification is available online) a protocol to ensure the interoperability of thing. Definition has been done with an integrative version with other protocols and considering the physical limitations of electronic devices.

Focusing on the NoT, each device has its application; e.g. *ZmotaAMBI* offers a tiny and low power sensor which is easily accepted by the user due to its low visual impact, easy installation and long battery lifetime. Thanks to its open firmware it can be used to add new devices to the system through its available expansion ports. Thanks to its inherent interoperability and openness it is also possible to create new services that interconnect devices. Inside NoT we propose CTP a protocol as an example

The modular architecture of the system based on an OSGi framework allows to easily add new virtual and real devices and functionalities, offering a remote maintenance, easy development of new services, etc.

All the software bundles have been also developed under open software licenses which will enable their use and modification by the community.

As future work, we plan to incorporate into the system new devices we are working on, such as more advanced sensors and tangible interfaces. We are developing NoTs that support *Things* with communications different to ZigBee. Currently we are working on developing modules such as *Zlita*, both for BLE (Bluetooth Low Energy) and Lora (Long Range). This is being addressed by designing several BEAGLEBONE-capes. Along with the development of hardware devices, it is also advancing interoperability with the new *Things* of these NOT. For which, CTP continues to evolve.

As improvements are done to the system, we are still looking for new project where it can be deployed, showings its capabilities and evaluating it during the trial. There have been proposals from institutional organism, such as the DGA (Diputación General de Aragon), to deploy the solution in public buildings to improve energetic efficiency and reduce the economic cost. This type of building systems usually have some kind of monitoring system, but in general they are local. Our system will be capable of connecting to them and collecting the information for conjoint analysis.

With all this, we intend to further research the capabilities of the WSN technology as the basis for the development of IoT.

Acknowledgments

This work is supported by *Renaissance* project.

References

- Alahmad, M., Wheeler, P.G., Schwer, A., Eiden, J. & Brumbaugh, A. 2012, "A comparative study of three feedback devices for residential real-time energy monitoring", *Industrial Electronics, IEEE Transactions on*, vol. 59, no. 4, pp. 2002-2013.
- Aman, S., Simmhan, Y. & Prasanna, V.K. 2013, "Energy management systems: state of the art and emerging trends", *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 114-119.
- Arnold, D., Sankur, M. & Auslander, D.M. 2013, "The next generation energy information gateway for use in residential and commercial environments", *Power and Energy Society General Meeting (PES), 2013 IEEEIEEE*, , pp. 1.
- Asensio, Á, Blasco, R., Marco, Á & Casas, R. 2013, "Hardware architecture design for WSN runtime extension", *International Journal of Distributed Sensor Networks*, vol. 2013.
- Asensio, Á, Marco, Á, Blasco, R. & Casas, R. 2014, "Protocol and Architecture to Bring Things into Internet of Things", *International Journal of Distributed Sensor Networks*, vol. 2014.
- Atzori, L., Iera, A. & Morabito, G. 2010, "The internet of things: A survey", *Computer networks*, vol. 54, no. 15, pp. 2787-2805.
- Barbato, A., Borsani, L., Capone, A. & Melzi, S. 2009, "Home energy saving through a user profiling system based on wireless sensors", *Proceedings of the first ACM workshop on embedded sensing systems for energy-efficiency in buildingsACM*, , pp. 49.
- BeagleBoard.org 2015, 2015/11/03-last update, *BeagleBoard Black - BeagleBoard.org - Community supported open hardware computers for making*.
- Byun, J. & Park, S. 2011, "Development of a self-adapting intelligent system for building energy saving and context-aware smart services", *Consumer Electronics, IEEE Transactions on*, vol. 57, no. 1, pp. 90-98.
- Chen, M. & Wu, C. 2012, "A ZigBee-based home control system using OSGi management platform", *International Journal of Smart Home*, vol. 6, no. 4, pp. 15-28.
- Cheng, S., Wang, C. & Horng, G. 2012, "OSGi-based smart home architecture for heterogeneous network", *Expert Systems with Applications*, vol. 39, no. 16, pp. 12418-12429.
- Ciuciu, I.G., Meersman, R. & Dillon, T. 2012, "Social network of smart-metered homes and SMEs for grid-based renewable energy exchange", *Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference onIEEE*, , pp. 1.
- Dong, Q., Yu, L., Lu, H., Hong, Z. & Chen, Y. 2010, "Design of building monitoring systems based on wireless sensor networks", *Wireless Sensor Network*, vol. 2, no. 09, pp. 703.
- Efergy 2015, 2015/11/03-last update, *Home Of Energy Monitors, Electricity Meters, Power Display*.

- Erol-Kantarci, M. & Mouftah, H.T. 2011, "Wireless sensor networks for cost-efficient residential energy management in the smart grid", *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 314-325.
- European Union initiative 2015, 2015/11/03-last update, *CONCERTO - European Union initiative*.
- Eurostat-European Commission 2011, "Energy, transport and environment indicators", .
- Froehlich, J. 2009, "Promoting energy efficient behaviors in the home through feedback: The role of human-computer interaction", *Proc. HCIC Workshop*, pp. 0.
- Globalscale Technologies 2015, 2015/11/03-last update, *GuruPlug Server - Globalscale Technologies*.
- Grilo, A.M., Chen, J., Diaz, M., Garrido, D. & Casaca, A. 2014, "An integrated WSN and SCADA system for monitoring a critical infrastructure", *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 3, pp. 1755-1764.
- Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. 2013, "Internet of Things (IoT): A vision, architectural elements, and future directions", *Future Generation Computer Systems*, , no. 29, pp. 1645-1660.
- Gungor, V.C., Lu, B. & Hancke, G.P. 2010, "Opportunities and challenges of wireless sensor networks in smart grid", *Industrial Electronics, IEEE Transactions on*, vol. 57, no. 10, pp. 3557-3564.
- Ha, Y. 2009, "Dynamic integration of zigbee home networks into home gateways using OSGi service registry", *Consumer Electronics, IEEE Transactions on*, vol. 55, no. 2, pp. 470-476.
- Han, D. & Lim, J. 2010, "Design and implementation of smart home energy management systems based on zigbee", *Consumer Electronics, IEEE Transactions on*, vol. 56, no. 3, pp. 1417-1425.
- Han, J., Choi, C. & Lee, I. 2011, "More efficient home energy management system based on ZigBee communication and infrared remote controls", *Consumer Electronics, IEEE Transactions on*, vol. 57, no. 1, pp. 85-89.
- Han, J., Choi, C., Park, W., Lee, I. & Kim, S. 2014, "Smart home energy management system including renewable energy based on ZigBee and PLC", *Consumer Electronics, IEEE Transactions on*, vol. 60, no. 2, pp. 198-202.
- HOWLab 2015, 2015/11/03-last update, *Zeta Project - OpenLab-HOWLab*.
- HOWLab-GEE 2015, 2015/11/03-last update, *Liga Energetica*.
- ISTAG 2015, 2015/11/03-last update, *ISTAG-Report-10-key-recommendations.pdf*.
- Kamstrup 2015, 2015/11/03-last update, *Contadores de energía térmica - Kamstrup*.
- Karaf 2015, 2015/11/03-last update, *Karaf 4.0.2 - The Apache Software Foundation*.
- Karlgren, J., Fahlén, L.E., Wallberg, A., Hansson, P., Ståhl, O., Söderberg, J. & Åkesson, K. 2008, "Socially intelligent interfaces for increased energy awareness in the home" in *The Internet of Things* Springer, , pp. 263-275.
- Kim, W.H., Lee, S. & Hwang, J. 2011, "Real-time energy monitoring and controlling system based on Zigbee sensor networks", *Procedia Computer Science*, vol. 5, pp. 794-797.
- Kulkarni, R.V., Förster, A. & Venayagamoorthy, G.K. 2011, "Computational intelligence in wireless sensor networks: A survey", *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 1, pp. 68-96.
- Kuzlu, M., Pipattanasomporn, M. & Rahman, S. 2012, "Hardware demonstration of a home energy management system for demand response applications", *Smart Grid, IEEE Transactions on*, vol. 3, no. 4, pp. 1704-1711.
- Lai, C., Ma, Y., Chang, S., Chao, H. & Huang, Y. 2011, "OSGi-based services architecture for cyber-physical home control systems", *Computer Communications*, vol. 34, no. 2, pp. 184-191.
- Lu, J., Sookoor, T., Srinivasan, V., Gao, G., Holben, B., Stankovic, J., Field, E. & Whitehouse, K. 2010, "The smart thermostat: using occupancy sensors to save energy in homes", *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems* ACM, , pp. 211.
- Marco, Á, Casas, R., Gerald, B., Blasco, R., Asensio, Á, Jean-Bart, B. & Ibañez, M. 2009, "Common osgi

interface for ambient assisted living scenarios" in IOS Press, , pp. 336.

Marinakis, V., Doukas, H., Karakosta, C. & Psarras, J. 2013, "An integrated system for buildings' energy-efficient automation: Application in the tertiary sector", *Applied Energy*, vol. 101, pp. 6-14.

Mirosa, M., Lawson, R. & Gnoth, D. 2013, "Linking personal values to energy-efficient behaviors in the home", *Environment and Behavior*, vol. 45, no. 4, pp. 455-475.

Moreno, M., Úbeda, B., Skarmeta, A.F. & Zamora, M.A. 2014, "How can We Tackle Energy Efficiency in IoT Based Smart Buildings?", *Sensors*, vol. 14, no. 6, pp. 9582-9614.

Nest 2015, 2015/11/06-last update, *The brighter way to save energy-Nest*. Available: <https://nest.com/>.

OSGi Alliance 2015, 2015/11/03-last update, *OSGi Alliance -Main / OSGi Alliance*.

Pachauri, R.K., Allen, M., Barros, V., Broome, J., Cramer, W., Christ, R., Church, J., Clarke, L., Dahe, Q. & Dasgupta, P. 2014, "Climate Change 2014: Synthesis Report. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change", .

Paganelli, F., Paradiso, F., Turchi, S., Luchetta, A., Castrogiovanni, P. & Giuli, D. 2015, "Appliance Recognition in an OSGi-Based Home Energy Management Gateway", *International Journal of Distributed Sensor Networks*, .

Paola, A.D., Re, G.L., Morana, M. & Ortolani, M. 2015, "SmartBuildings: an Aml system for energy efficiency", *Sustainable Internet and ICT for Sustainability (SustainIT)*, 2015IEEE, , pp. 1.

Pérez-Lombard, L., Ortiz, J. & Pout, C. 2008, "A review on buildings energy consumption information", *Energy and Buildings*, vol. 40, no. 3, pp. 394-398.

Ramos, C., Augusto, J.C. & Shapiro, D. 2008, "Ambient Intelligence—the Next Step for Artificial Intelligence", *Intelligent Systems, IEEE*, vol. 23, no. 2, pp. 15-18.

Renaissance 2015, 2015/11/03-last update, *Renaissance Project*.

Robinson, D., Sanders, D. & Mazharsolook, E. 2014, "Sensor-based ambient intelligence for optimal energy efficiency", *Sensor Review*, vol. 34, no. 2, pp. 170-181.

Rodrigues, J.J. & Neves, P.A. 2010, "A survey on IP-Based wireless sensor network solutions", *International Journal of Communication Systems*, vol. 23, no. 8, pp. 963-981.

Saveometer 2015, 2015/11/04-last update, *Saveometer Personal Smart Meter*.

Schwartz, T., Stevens, G., Jakobi, T., Deneff, S., Ramirez, L., Wulf, V. & Randall, D. 2014, "What People Do with Consumption Feedback: A Long-Term Living Lab Study of a Home Energy Management System", *Interacting with Computers*, , pp. iwu009.

Song, E.Y. & Lee, K. 2008, "Understanding IEEE 1451-Networked smart transducer interface standard-What is a smart transducer?", *Instrumentation & Measurement Magazine, IEEE*, vol. 11, no. 2, pp. 11-17.

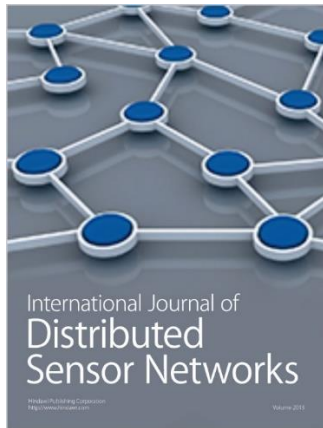
Specification, Z. 2008, "ZigBee cluster library specification", *053474r17*, .

Sundramoorthy, V., Cooper, G., Linge, N. & Liu, Q. 2010, "Domesticating energy-monitoring systems: Challenges and design concerns", *IEEE pervasive Computing*, , no. 1, pp. 20-27.

U.S. Energy Information Administration 2015, 2015/11/03-last update, *Annual Energy Review 2011 - Energy Information Administration*.

Zhengguo Sheng, Shusen Yang, Yifan Yu, Vasilakos, A., McCann, J. & Kin Leung 2013, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities", *Wireless Communications, IEEE*, vol. 20, no. 6, pp. 91-98.

2.3 PROTOCOL AND ARCHITECTURE TO BRING THINGS INTO INTERNET OF THINGS



Ángel Asensio, Álvaro Marco, Rubén Blasco, Roberto. Casas.
 International Journal of Distributed Sensor Networks
 Article ID 158252, doi: 10.1155/2014/158252.

2014

RESUMEN:

En este trabajo se realiza una revisión de la arquitectura de IoT y una modelización de las Cosas acorde a sus usos y requisitos. A raíz de lo anterior se analiza y pone en contexto la problemática de la interoperabilidad entre las Cosas. Se consideran los distintos niveles implicados, desde las capas inferiores de la comunicación hasta la abstracción del conocimiento, realizándose una revisión de diferentes propuestas. Junto a la eficiencia energética, “Manuscrito 1 (Eficiencia HW)”, la interoperabilidad es otro de los retos que deben superar las Cosas de IoT. Por ello, considerando las alternativas más óptimas se propone CTP como protocolo para articular la interoperabilidad entre las cosas. CTP supone una de las principales aportaciones de esta tesis, por lo que es ampliamente descrito en este manuscrito. Se continúa abordando la implementación práctica de CTP en una arquitectura basada en Gateway que lo integra con IoT. Los avances presentados en este manuscrito se han implementado en los desarrollos prácticos comentados en el “Manuscrito 2 (IoT Energy Awareness)”. A raíz de éstos, se comprobó la necesidad de disponer de herramientas para evaluar la calidad de las propuestas e implementaciones. Por ello, este manuscrito también aborda la problemática de las métricas y factores de calidad.

Research Article

Protocol and Architecture to Bring Things into Internet of Things

Ángel Asensio, Álvaro Marco, Rubén Blasco, and Roberto Casas

Aragon Institute of Research, University Zaragoza, 50018 Zaragoza, Spain

Correspondence should be addressed to Álvaro Marco; amarco@unizar.es

Received 1 December 2013; Revised 16 February 2014; Accepted 16 February 2014; Published 13 April 2014

Academic Editor: Zuqing Zhu

Copyright © 2014 Ángel Asensio et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Internet of Things (IoT) concept proposes that everyday objects are globally accessible from the Internet and integrate into new services having a remarkable impact on our society. Opposite to Internet world, *things* usually belong to resource-challenged environments where energy, data throughput, and computing resources are scarce. Building upon existing standards in the field such as IEEE1451 and ZigBee and rooted in context semantics, this paper proposes CTP (Communication Things Protocol) as a protocol specification to allow interoperability among *things* with different communication standards as well as simplicity and functionality to build IoT systems. Also, this paper proposes the use of the IoT gateway as a fundamental component in IoT architectures to provide seamless connectivity and interoperability among *things* and connect two different worlds to build the IoT: the *Things world* and the *Internet world*. Both CTP and IoT gateway constitute a middleware content-centric architecture presented as the mechanism to achieve a balance between the intrinsic limitations of *things* in the physical world and what is required from them in the virtual world. Said middleware content-centric architecture is implemented within the frame of two European projects targeting smart environments and proving said CTP's objectives in real scenarios.

1. Introduction

Since the last decade, we are assisting in a progressive jump from a nonubiquitous Internet, where humans access Internet using a computer at their work or at home, to the current ubiquitous Internet where we access the Internet using smartphones, tabs, or TVs, anytime, anywhere. In the same way, now comes the time of the Internet of Things (IoT) when not only humans but also *things*, any object surrounding us, are present in Internet [1].

Things must be considered in the broadest sense of the word as real or virtual entities that exist and evolve in a context and time and have univocal identifiers. On the other hand, the term Internet applied to them conveys the idea that all these *things* are heavily communicated and interrelated among them. Commonly IoT can be approached from different perspectives: *Internet* for communications, cloud, and services; *things* for physical elements, sensor networks, and user interfaces; and *semantic* that considers ontology of *things* in Internet [2].

Ideally, *things* on the IoT will have full interconnectivity and computation resources, being natural to consider connecting these *things* to the web using current paradigms. Different works investigate the types of *things* (sometimes called smart objects), their nature, and relationship with the IoT; according to the different perspectives, a *thing* has awareness, representation, interaction, and so forth [3]. The classification of *things* into standard groups helps to show that they are the physical part of IoT with constraints and needs that must be taken into account. So, coming down to implementation, while IoT concept talks about ubiquitous, invisible, and context aware *things*, technology poses hurdles such as energy supply, price and size of devices, seamless connectivity, or interoperability [4]. Additionally, as, currently, Internet has a wired backbone, "being there" forces all the *things* to be IP compatible and use access points or gateways to bridge global fiber optic or cabled infrastructure.

Wireless communication protocols are mandatory if *things* need to be mobile and ubiquitous. Depending on the specific application, and leaving aside proprietary protocols,

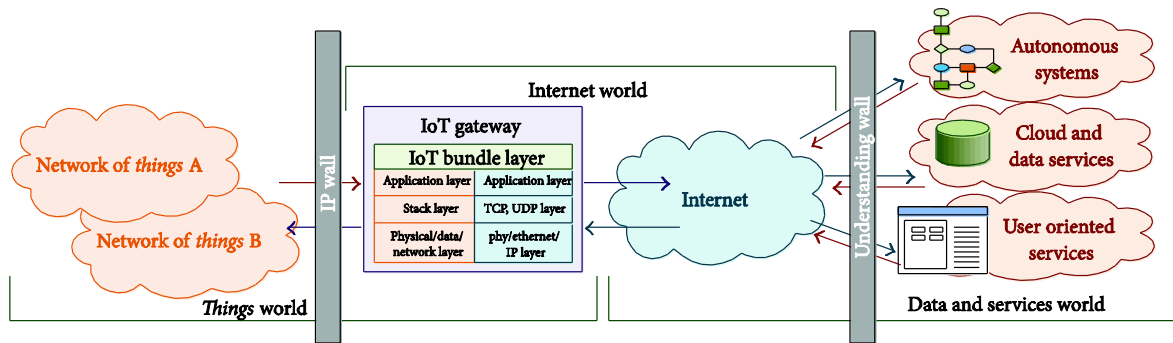


FIGURE 1: IoT architecture.

different standards are commonly used to provide connectivity: ZigBee, RFID, Bluetooth, 6lowPAN, WIFI, 3G, and so forth. Many works evidence the importance of selecting the most appropriated technology in each situation comparing them in terms of network topology, coverage, data throughput, or energy consumption. In any case, the more data you need to exchange, the further you need to communicate, the more time you need to be online, then more energy you need, and consequently the quicker you will run out of batteries.

The arrival of IoT will lead to appearing multitude of new services, improving the quality of life of people, and offering new business opportunities. Ultimately, the IoT is expected to bring a revolution in the concept of society, similar to how Internet changed the concept of communications and information [5]. In the last few years, initiatives and project related with IoT have been growing in number and scope throughout the entire world. The IoT concept is becoming tremendously popular and already appearing systems that claim to offer IoT solutions to the final user without high technical requirements [6]. Current developments are in early stages being most of the services based on monitoring or sensing variables to extract information and then analyze and represent them [7].

It is considered that the development of IoT will play an important role in the near future; thus, public and private investments have been made in R&D, demonstration, and deployment activities [8, 9]. To date, most of IoT solutions are small subnets of interconnected objects. It is not possible to talk about IoT until all objects are interconnected and to improve this interconnectivity, an architecture that ensures interoperability between systems is mandatory. Thus, both public and private initiatives are currently focusing on standardization of the IoT [10–14].

In summary, the evolution of IoT implies overcoming real *things*' limitations enabling them to communicate with the Internet using a common language. In this paper, we propose CTP (Communication *Things* Protocol) as an ontology-based solution to enable understanding among *things* and the use of an IoT gateway to take *things* to the Internet world.

2. Internet of Things

2.1. Architecture. Most IoT implementations follow an architecture that contains different worlds each of them with their own characteristics; Figure 1 shows an example [15].

The *things* world relates to microelectromechanical systems, smart sensors, simple human-machine interfaces (HMIs), and so forth, which associate in networks (Networks of *Things*, NoT) to ubiquitously interact with other *things*, the environment and/or people. NoT are usually resource-challenged ecosystems, typically with medium-high time access delays, high error rates, low data throughput, and limited online time where energy consumption must be optimized to the maximum. In a simplified model of a *thing*, basic blocks of communication, computation, and interaction (sensors, actuators, and HMI) are distinguished.

The Internet world usually is constructed around computers, centralized software infrastructures, or in the cloud [16]. Applications and services use *things* to provide context awareness, artificial intelligence, affective computing, and so forth [16]. Depending on their consideration, tablets and smartphones can be included in both worlds. Nevertheless, due to their power (computing, communications, battery lifetime, user interfaces, etc.) we find it more appropriate to consider them closer to the world of computers and Internet than to the world of *things*. Currently, Internet acts as the base infrastructure for the exchange of information. However, access to it has several constraints such as the need for unique identifier, the change of communication technology, and the adoption of the Internet Protocols. Nowadays, this "IP wall" is usually jumped through an IoT gateway.

Internet is the global interconnection method where multitude of services and applications use extracted information of IoT to provide services to end users. On each of them, needs are a virtual representation of the *things* of the IoT in order to enable interaction. Once "IP wall" is saved and thanks to the connectivity provided by the Internet, services can access the information, but, for the information to be useful, it must be understood and this poses what we call the "understanding wall."

2.2. Interoperability. IoT interoperability implies capacity to both exchange data (crossing the IP wall) and understand the information embedded in data (crossing the understanding wall). Communication standards ensure stack layer's communication between *things* in the same network sharing the same protocol, that is, network management and maintenance, security, data exchange, and so forth. Nevertheless, if application layer is not defined, *things* will not understand among them unless previously agreed between developers, that is, information understanding. This is the case of 6lowPAN, RFID, WiFi, or cellular; for example, if two manufacturers want to develop 6lowPAN temperature sensors and thermostats are able to interoperate among them, there is no common definition to adopt; they will need to agree on the protocol exchange application-related information, temperature data format, procedure to virtually bind devices, and so forth.

Automation and control networks such as Lonworks, BACnet, Konnex, or CANOpen define how devices are represented in their networks; objects and variables are the most common approaches. Bluetooth and ZigBee go one step further in interoperability defining profiles and device objects within the application layer. Bluetooth defines profiles (hands-free, health device, human-interface device, etc.) corresponding to vertical applications. For example, we could build a monitoring infrastructure with Bluetooth microphones streaming audio according to hands-free profile; no matter their manufacturer, any certified host compliant with the profile will play the audio gateway role without any additional programming [17].

ZigBee not only defines vertical profiles (home automation, energy metering, healthcare, etc.), but also defines horizontal functional domains to specify how devices must exchange application data attending their functionality [18]. For example, every ZigBee compliant temperature sensor must implement "measurement & sensing functional domain" and any other device in the network (e.g., a thermostat) would be able to get temperature information as defined in the specification. Additionally, ZigBee allows instantiation of intelligence in the network by defining how to coordinate devices to produce scenes and create virtual bindings among devices [19], for example, to program a switch to turn on two lights and open a motorized door.

Sometimes two specifications coordinate to solve interoperability, such as ZigBee that specifies how to interoperate with BACnet. Devices using any wireless communication standard (e.g., ZigBee) cannot directly interoperate with devices over other standards (e.g., WiFi) unless there is a protocol aggregator and translator connecting both worlds, the IoT gateway.

Although IP connectivity is not necessarily required to ensure inter-*thing* communication, many standards include IP as part of their specification to ease the process to connect *things* to the Internet. Nevertheless, this is not enough to ensure interoperability at required IoT application level. As *things* are resource-challenged communication nodes, efficient data transmission mechanisms are needed at IP level; CoAP [20], XMPP [21], RESTful HTTP [22], and MQTT are relevant specifications at this level.

Once efficient connectivity between devices is granted, standards such as EEML (Extended Environments Markup Language), SensorWeb (including SensorML and TransducerML), or SenseWeb provide interpretation to bytes exchanged integrating sensors and actuators with the virtual world. These schemes just express queries and data modeling, lacking of semantics, and ontologies that are necessary for complex information processing and support to service composition and adaptation at higher levels of abstraction.

IEEE1451 standard is a network-independent specification for smart transducers (sensors or actuators) that provides a common language regardless of the protocol used. The standard defines different application profiles: environmental (climate monitoring, greenhouse gases, and other chemical sensors), smart meter (monitor water, gas, or electricity consumption), health care (monitor the body using external or implantable sensors), and smart home automation and industrial (pipe's monitoring, comfort, and surveillance sensors) [23]. The standard is based on the Transducer Electronic Data Sheet (TEDS) to describe a set of communication interfaces for connecting transducers to microprocessors, instrumentation systems, and control/field networks. According to IEEE1451.0 specification, TEDS provides information about transducer's identification, operation, calibration, manufacturer, and so forth.

Lying on IEEE1451.5 specification for radio-specific protocols [24], it is possible to implement wireless sensor networks using IEEE1451 over communication standard protocols such as Wifi [25], Bluetooth, ZigBee [26], or 6LowPan [27]. Similarly, IEEE1451.2 defines cabled SPI and UART, IEEE1451.6 over CANOpen, and IEEE1451.7 over RFID. This interoperability is enabled by the Network Capable Application Processor (NCAP) that aggregates the different Transducer Interface Module's communication standards (TIM) over the same common language. Through NCAP and following IEEE1451 it is possible to implement web services that make *things* discoverable, accessible, and controllable via the Internet [22]. In the same line, ZigBee defines the ZigBeeGateway Public Application Profile that specifies how devices must be connected to the Internet and to service providers.

Initiatives, such as Sensei project [7], COSE [28], DogOnt [29], and other [30] different ontological approaches to model *things* (sensors, actuators, simple human-machine interfaces, appliances, etc.) in smart environments, associate contained devices through semantic relationships [31] and seamlessly integrate *things* with web services.

3. Common Things Protocol (CTP)

3.1. Rationale. Networks of *things* (NoT), defined as smart infrastructures of embedded devices with local intelligence and access to the "information ether," are the base of the IoT. As a part of the Internet, one of the basic needs is the interaction mechanism between agents which implies that, between them, there must be connectivity and understanding in order to provide interoperability. To achieve this goal, different IoT protocols are being proposed to provide efficient,

seamless, and robust connectivity (CoAP, XMPP, RESTful HTTP, MQTT, etc.) but not providing semantics. From an integral perspective, IEEE1451 appears to be a good suited option for the IoT as it tackles specification from sensor to network interface providing independence from the communication protocol, enabling self-identification of devices, long-term self-documentation, plug and play capacity to ease field installation, upgrade, and maintenance [32]. On the other hand, the standard has a limited penetration in IoT applications out of the electronic instrumentation field. Reasons for that can be the little compatible hardware available (no commercial wireless sensor networks consider it) because IoT developers mainly come from the computer science field (usually considering semantic approaches), due to complexity of the standard [33], or the excessive detail in electronic aspects that are not commonly used by the application (e.g., transducer channel reads delay time or incoming propagation delay through the data transport logic). Communication standards such as ZigBee or 6LoWPAN are much more used in IoT applications but involve hardware restrictions and lack of interoperability among them.

The Common Things Protocol (CTP) aims to provide a specification that allows interoperability among communication standards and coexistence with IoT protocols, but prioritizing simplicity, efficiency, and functionality to build final IoT systems.

CTP takes into consideration existing specifications in the standards and the needs from the final applications that are to be supported by the *things* in the field. It integrates the strategies, concepts and terms of some of the alternatives, for example, IEEE1451 TED's concept to provide device's information, sensor and actuator working modes, and so forth, or ZigBee concepts of clusters and endpoints. CTP definition is approached from an ontological perspective considering *things*, not just as sensors [34] but as electronic devices that perform some sort of function in the IoT application being in contact with user and context and usually fulfilling the following paradigms:

- (i) *context interaction*: embedded sensors (to sense the user/context), actuators (to modify the environment), and/or simple human interfaces (to interact with people);
- (ii) *computin*: to have computing capabilities and memory that allow them to implement from the simplest logic to complicated services or data processing algorithms;
- (iii) *communication*: to have at least one, usually wireless, communication media commonly following a standard and adapted to communication requirements (range, power consumption, and data throughput). It is required to interoperate among them and integrate in the Internet. Thus, unless they are able to directly connect to Internet, a network gateway is required to allow interoperability among different networks of *things* and to provide Internet access;
- (iv) being an *electronic thing*: as anything in this world, regardless it is electronic or not, each *thing* is unique

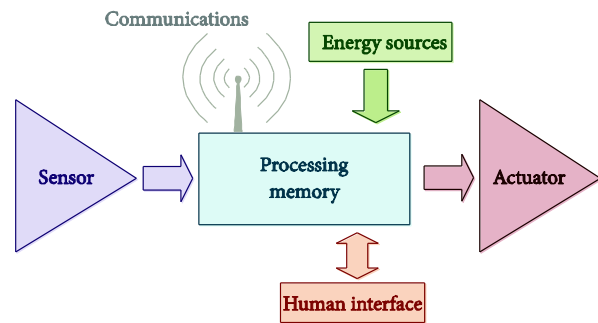


FIGURE 2: *Thing* block diagram.

and “lives” in a specific space and time. Additionally as any electronics, it needs energy to operate.

Figure 2 represents said paradigms in the block diagram of a *thing* able to integrate in the IoT.

Thus, derived from their capacity to interact with the context, CTP considers that *things* can have three different functionalities:

- (i) sensors that gather and process information from the real world in environmental and person-centric contexts [35]. Information from the environmental context is useful to create an objective snapshot of what is happening in every moment, while person-centric helps to understand and evaluate the objective data in order to extract conclusions, to define guidelines, or to identify patterns adapted to each user;
- (ii) actuators that provide the ability to act over the environment. IoT applications may need to act over the environment when the user is not able to control (e.g., because he/she has a disability) or he/she is not aware of specific situations that require actuation (e.g., forget about the heating when going to sleep) or simply he/she is not present in the environment;
- (iii) pervasive human-machine interfaces including traditional (switches and dimmers) and new interaction paradigms, providing the user with relevant information or notifying him/her about events in new and natural ways (e.g., a color device turns red when house's energy consumption is high).

Regardless its functionality, each *thing* will always “live” in a certain location and time and will have a processor, communication transceiver, and power source. Similar to MetaTEDS in IEEE1451 and ZigBeeDevice Object (ZDO) in ZigBee, this constitutes the basic set of attributes and functionalities of any device, which is modeled by the endpoint BASE in CTP. Depending on the specific functionalities it integrates, it will also implement multiple application endpoints that should be of any of the said categories: SENSOR, ACTUATOR, or HMI.

Thus, an endpoint can be defined as each of the sub-devices that have a complete functionality and together with others build the *thing*; in total we just define the said 4 endpoints to model *anything*. Additionally, a cluster is defined

as a set of commands, events, and responses (some mandatory to implement in order to guarantee interoperability) which together define a communication interface between two endpoints. Clusters constitute the implementation of the ontological representation of *thing's* nature; for example, endpoint BASE includes location, time, and power clusters. Endpoint and cluster concepts are shared with ZigBee and are similar to transducer channels in IEEE1451.

Commands are usually action requests to an endpoint (of the same or different *thing*) that should send back a response informing about the action result, for example, ask for a sensor value and get it back. The ontology defines attributes which are implemented in the protocol as GET/SET requests and responses. Events are asynchronously generated messages sent to previously subscribed endpoints; for example, presence detected by a sensor is sent to light actuator. When defining a communication interface, two strategies can be adopted: (i) using a small, but well defined, number of messages, where the versatility is achieved by parameters (ii) or defining a greater number of messages allowing more specific control with lower parametric content [36]. An example of this duality is to define a single configuration command with many parameters, or several commands to adjust each parameter independently. The selection of one or another philosophy conditions ease of use, generalization capacity, adaptability to different scenarios and future maintenance, and backwards compatibility. CTP chooses to define a reduced and simple communication interfaces defining the meaning type and range of the parameters when needed. For example, many clusters have in common a read-only information attribute; in the case of sensors it provides information of ranges, accuracy, format, units, and so forth of the measure it provides, while for actuators the same attribute indicates how the actuator should be controlled. Similarly, some clusters include a read-and-write configuration attribute, whose specific parametrization depends on the device.

3.2. Endpoints and Clusters. Figure 3 shows the four endpoint types (BASE, SENSOR, ACTUATOR, and HMI) with their associated clusters and the main attributes, commands, responses, and events.

3.2.1. Endpoint BASE. All devices, regardless their nature, must have endpoint BASE containing the generic and common characteristics whatever their functions are. Related with this endpoint we define the following clusters.

Cluster DEVICE. It manages *device identification, description* of their functionalities (as in IEEE1451 TEDS's globally unique identifier and transducer channels), and *minimum self-operation* functionalities (as BIOS). Its implementation is mandatory in all CTP devices, as it is the basis for ensuring interaction with other system elements. Devices may have the ability to operate in different ways depending on the context; the *mode* parameter is used to switch between them and to facilitate the use of the *thing*, by providing to a nonadvanced user a set of predefined modes of operation that do not

need any previous settings to set mode and operate. Also, this cluster has several capabilities oriented to work with low power devices, for example, and similar with TEDS, a *timeout* parameter that indicates the amount of time after an action for which the lack of reply following the receipt of a command may be interpreted as a failed operation.

Cluster LOCATION. Each device will always have a location that can be essential information for many services. It can be known or not, it can change or remain, and device can self-calculate it or be written externally, whichever the case, this cluster allows getting and setting *device's position*, programming its timed update, or reporting it in response to specific events.

Cluster POWER. As location, every device will have a *power source* (battery, mains, energy harvesting, etc.); its type, consumption profile, and energy remaining are the main information deal within this cluster.

Cluster TIME. Again as location and power, every device "live" in a specific instant of time, and whether relative or absolute this cluster allows the management of temporal information such as time synchronization and scheduling of timed actions.

Cluster PROXY. Similar to TEDS, this cluster acts as an aggregator of endpoints (or transducer channels) and datalogger manager (if memory is available) simplifying access to data. It reduces communication burden and thus increases battery efficiency.

Often, implementation of networks of smart sensors and actuators goes through a central device that receives data from sensors, processes the information, and then orders actions to the actuators. This has a number of problems: (i) density of data traffic, (ii) increased energy consumption, (iii) masking the mesh concept, since there is a central node acting as sink and source of information, and (iv) reducing robustness to failure. To face that, it is possible to define a basic distributed intelligence by subordinating the behavior of some devices to the events generated by other devices.

Cluster BEHAVIOR. Similar to ZigBee this allows the creation of groups of devices or endpoints and the establishment of logical relationships (bindings) among them. We expand its native definition defining the concept of a trigger event for a *binding* which allows that any endpoint generating events (e.g., timing, threshold event, etc.) could trigger any endpoint(s) in one or more devices with their corresponding parameters (e.g., changing the mode to low power of a device). Also, as in TEDS when defining embedded actuators, these bindings can be internal to a device and serve, for example, to trigger actions; button event triggers a light actuator.

This cluster also allows delegation of system's intelligence in the devices as it provides methods to program autonomous operation based on the specification of operational rules. It is based on logical rules that verify compliance with certain conditions of different endpoints of the device. Each situation



FIGURE 3: Summary of endpoints, clusters, and main interfaces in CTP.

that activates a behavior is called activation scenario. Notice that as a result of a rule of behavior a binding could be triggered.

3.2.2. *Endpoint SENSOR*. Sensors are elements that can extract information from the context. CTP allows management of basic features and supports more abstract and complex capabilities.

Cluster SENSOR. As transducer channels TEDS, it manages the basic actions to request measure, defines sensor settings (e.g., sampling period), and defines the mode for transmitting the data set or data packets aggregating several measurements (e.g., on command, timed, or buffer full). It also provides essential attributes of the measurement such as units, accuracy, data ranges, warm-up time, vectors, and data packets. Every sensor type must implement this cluster.

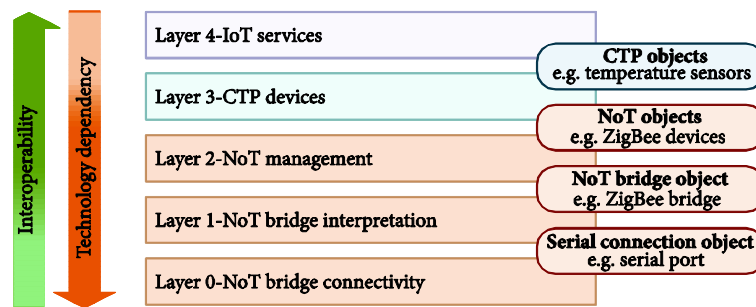


FIGURE 4: IoT gateway middleware architecture.

Cluster SENSOR_EVENT. Again as transducer channels TEDS it configures event triggers associated with a sensor (e.g., upper and lower thresholds, bit patterns, etc.) and provides the events.

Cluster SENSOR_STATS. This cluster performs local preprocessing and analysis of the captured data. This is of special interest when we are interested in obtaining a summary of the observation (e.g., maximum values, average values, etc.). As energy consumption between communication and computation in a wireless sensor node has a high ratio (“sending one bit” versus “computing one instruction”) [37], its implementation is especially interesting in low power applications.

3.2.3. Endpoint ACTUATOR. While sensors allow obtaining contextual data, actuators are the elements that provide means to act over the environment. In relation with the IoT, an actuator can be considered as a device that transmits information or energy to another power mechanism or system (motors, electromagnets, thermocouples, heaters, coolers, etc.) that finally alters the environment. Thus, a *thing* with actuation capabilities is usually a device with control outputs, which is connected to an electromechanical system that opens doors, windows, shutters, control lighting, heating, and so forth.

Cluster ACTUATOR. It manages basic actions, controls the states of the actuator, and defines its configuration parameters. These states can be as simple as on/off or define complex operation patterns such as open the door for two minutes and then close and lock it.

3.2.4. Endpoint HMI. HMI (Human Machine Interface) devices are aimed to interact with a human user. In fact, they could be considered as sensors and actuators to interface people (in the same way that sensor and actuator connect with the environment). But given its importance and different use from the application perspective, it is convenient to assign its own type of endpoint. CTP considers the following clusters.

Cluster HMI_INPUT. It manages configuration and operation of simple input devices interface, such as buttons, switches, or

dimmers. It also considers groups of elements such as arrays of keys to model a keypad.

Cluster HMI_OUTPUT. It manages basic operation of simple output devices such as LEDs and buzzers. It also considers groups of elements such as arrays of LEDs to model a LED strip.

4. IoT-Gateway Architecture

According to the proposed architecture, the different *things*, maybe on several NoTs, must interconnect to the Internet, that is, jumping to the IP world. In most cases, this involves changing not only the communications protocol but also communication technology, which imposes the need of a gateway interfacing *things* and Internet worlds.

In the proposed architecture, the gateway is not a single bridge between protocols; it is also an intelligence aggregator and distributor of services. The IoT gateway must support management (discovering, recruiting, and connecting devices) in the NoTs and provide interoperability between them. Such duty requires that the IoT gateway have enough power computation to handle requests and responses from both domains and a flexible architecture to ensure interoperability. To accomplish such task, the layered middleware architecture shown in Figure 4 is proposed.

Lower layer of the middleware is in charge of providing base connectivity with the NoT through the device acting as the network bridge, typically a USB dongle, a Bluetooth device, or a TCP socket which results in a sort of serial connection object allowing sending and receiving bytes as data streams.

Second layer adds meaning to those bytes, implementing the specific communication protocol of the bridge and allowing effective communication with the NoT. This results in an object representing the bridge, which encapsulates the communication protocol with appropriate methods and fields.

Middle layer is in charge of managing the NoT through the usage of the bridge representation service, being capable of discovering network devices (*things*), recruiting them, and handling network unavailability. At this layer, objects representing network devices are available, although they are already described in terms of the underlying technology.

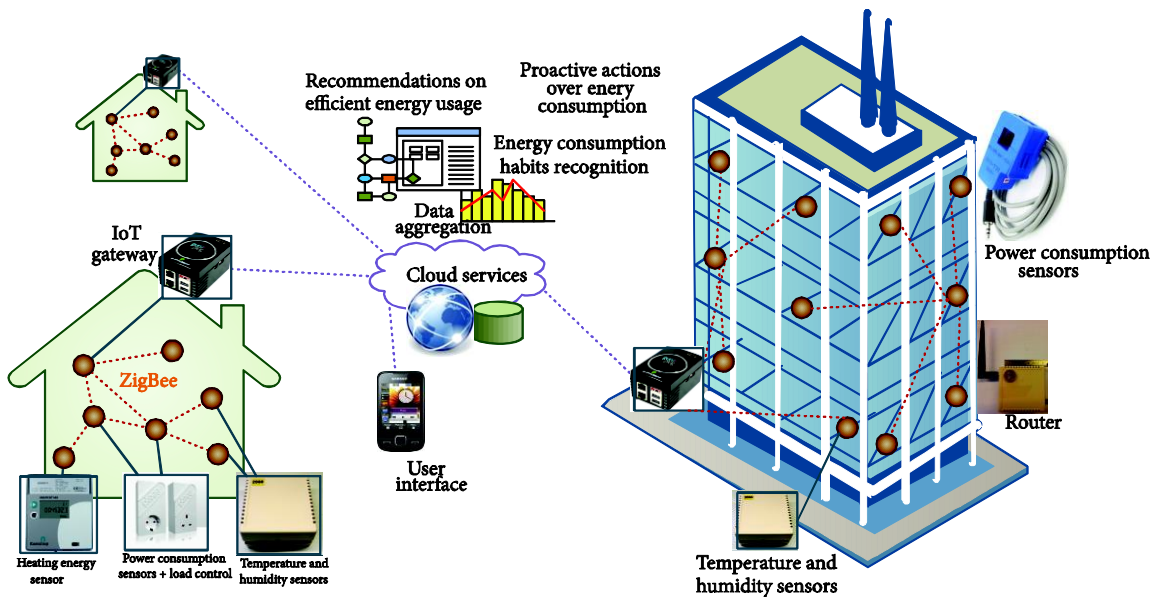


FIGURE 5: Test scenarios.

In the next layer, objects related to NoT devices are described as CTP objects, regardless their network technology, and full interoperability among *things* is achieved. CTP objects are described as a main device representing the endpoint BASE plus a collection of *channels* related to remainder endpoints.

Upper layer is devoted to gateway IoT services, which use CTP objects to link them to remote services (such as sending data to a remote database or allowing accessing a *thing* from a remote client) or build local services to perform offline operations.

5. Experimentation and Results

CTP has been successfully applied in several projects, but the largest implementations have been done in two European projects: “Easy Line Plus” [38] in the domain of Ambient Assisted Living and “Renaissance” [39] in the domain of Energy Efficient Buildings. The Easy Line Plus project sets the frame to define the CTP protocol, but it was within the Renaissance project where all the aspects described above have been formally deployed and tested. Therefore, we will describe below the Renaissance project setup.

5.1. Test Scenario. “Renaissance” main objective is energy saving, through the implementation of bioclimatic buildings, urban planning and rehabilitation, incorporating renewable energy, and reduction of energy consumption in households by improving habits of energy usage by users. Through remote data analysis, the system derives user patterns relating their energy consumption and comfort variables and then issues recommendations in order to increase their awareness and enhances energy savings. This requires an accurate and

long-term monitoring of energy consumption and environmental conditions in order to generate enough data to extract relevant information.

To meet the needs of this project, the IoT paradigm is the ideal solution. The simplified structure of the system is a number of *things* that ubiquitously extract context information (temperature, humidity, heating energy, and power consumption). Through the proposed architecture, this information is handled (data aggregation, data base management, and cloud computing) and analyzed (habits recognition) to provide a range of services (data visualization, user profiling, assessment of the best practices, and user information through multimodal user interfaces).

Technically the system developed followed the architecture in Figure 1; *things* use ZigBee standard plus CTP; IoT gateway is a Linux embedded PC running the already presented middleware, and services run in different hosts (PC, mobile phones) using data stored in the cloud. As evaluation has been done in a real and operative deployment, the system previously ensured a number of quality requirements such as stability, ease of deployment and maintenance, and low intrusiveness in the context. Similarly, a number of limitations related to the *things* have been solved, namely, reducing power consumption to ensure months of operation with the same batteries, cost-effectiveness, and reduced size.

Two different types of installations have been done as follows (Figure 5):

- (i) 80 m² dwellings with one ZigBee network formed by 3 ambient (temperature + humidity) sensors, 1 heating energy sensor, 1 monophasic power consumption sensor, and an IoT gateway;
- (ii) 20.000 m² building with one ZigBee network formed by 70 ambient sensors, 20 triphasic power consumption sensors, 17 routers, and an IoT gateway.

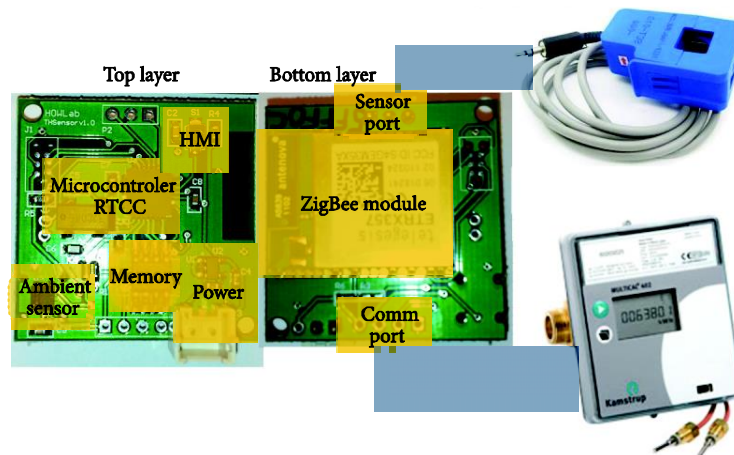


FIGURE 6: Zigbee *thing* hardware implementation.

In both cases, although the environment is quite different, the technological development is similar, allowing assessing and evaluating CTP in different scenarios.

The system has been installed and was running for 9 months in 43 dwellings simultaneously (i.e., 43 systems) in Zaragoza, proven to be stable, no maintenance was needed, and the expected functionality was provided. The building installation has been running for 6 months (already running) at the University of Zaragoza [40].

5.2. ZigBee Network of Things. Besides forming a ZigBee network, the sensors developed allow sensing the physical environment, connecting to analog or digital simple external sensors (e.g., presence detector, magnetic contact, etc.), and connecting to external commercial smart meters (e.g., commercial electricity or heating water consumption).

The aforementioned 20.000 m² building with long corridors, anti-fire doors, and so forth is a challenging scenario for wireless communication network with a hundred of nodes. A multihop mesh topology with an overlap of coverage areas and redundant communication paths was deployed. The ZigBee network backbone is formed by 17 routers, 1 network coordinator, and a data sink connected to the IoT gateway. The infrastructure is devoted to keep routing tables to date and interconnect 90 CTP *things* (70 ambient sensors and 20 power consumption sensors) that are ZigBee Sleepy End Devices. Any sensor enters low power mode between measurements, being disconnected from the network along this time, and its *father* (a router) holds its messages. Periodically, sensors poll their parents to check for incoming messages. This time between polls introduces latency in the communication but reduces energy consumption of the *thing*; to avoid possible loss of messages it is set to 4 seconds. Also, time between measurements, time between sending data, timestamping, and so forth can be configured in order to balance power consumption and application requirements. In this application, environmental nodes measure and immediately send data every 10 minutes,

while power consumption sensors measure and store data every minute and then send it every 10 minutes. As it is not necessary that measures are simultaneous, the update process of the system is randomized to reduce the probability of several *things* trying to send messages at the same instant, which would increase medium access time and, therefore, energy consumption.

5.2.1. Hardware. Hardware implementation (Figure 6) is designed to be versatile. Device implementation is based in a dual hardware architecture where a low power microcontroller (PIC18F26J11) runs the main application and controls the network coprocessor that implements ZigBee Pro stack (Ember 357). After deep analysis and experimentation, we found architecture more efficient in terms of power consumption than using a system on chip solution (embedding a radio module plus a programmable microcontroller) as it allows splitting tasks between two specialized microcontrollers, one for sensing and processing tasks and the second for communication [41]. The device additionally has an EEPROM memory, a real time clock, expansion ports, a button, a LED, and a temperature and humidity digital I2C sensor (Sensirion SHT21). Along with these onboard capacities, the hardware features two expansion ports: first for connection of external analog/digital sensors and second for communications to external systems. Thanks to them, different *things* are built: a noninvasive AC current sensor (a SCT-013-000 0-100A split core current transformer) enables power consumption sensor and a communication port connected to a commercial device (Kamstrup) for measuring heating water consumption.

5.2.2. Firmware. Accordingly, the basic configuration of the device (only onboard capabilities) presents 5 endpoints: base (base type), temperature (sensor type), humidity (sensor type), button (HMI type), and LED (HMI type). Note that although SHT21 sensor is a single electronic component that measures temperature and humidity, there are two different endpoints one for each magnitude.

Nevertheless, similar to IEEE1451, access to both endpoints is possible using the proxy cluster within the base endpoint. According to the devices connected to the ports described above, new endpoints (power and heating water consumption, both sensor types) are added when necessary. The CTP protocol is therefore suited to the different characteristics of the hardware, while performing an abstraction of it.

Clusters implemented per endpoint are as follows:

- (i) BASE: device, power (for battery level monitoring), time (to provide timestamps), proxy, and behavior (to program clima control when event happens),
- (ii) SENSOR: sensor (to provide single measurements), sensor event (to get events when upper and lower thresholds are surpassed), and sensor stats (to provide maximum and minimum levels),
- (iii) HMI: HMI input (to handle button events) and HMI output (to handle LED operation).

The use of CTP provides a structured and simple programming strategy, which results in modular code with high reusability. Figure 7 shows a simplified view of the proposed structure for a common firmware of a *thing*: configuration of the microcontroller, peripherals, ZigBee communications, and CTP and system behavior.

5.3. IoT Gateway. An embedded computer running Linux, where the middleware described before was implemented, acts as the IoT gateway. The middleware architecture falls within the SOA (Service Oriented Architecture) paradigm, and we use OSGi [42] (Open Services Gateway initiative) as development framework. OSGi defines a framework where pieces of code are organized into bundles that can be managed separately. OSGi bundles are agents which might be dedicated to specialized tasks, such as handling a serial port, providing a command line interface, collecting, aggregating and analyzing data, and so forth. These bundles communicate and interact with each other by means of services which are published within the framework, and each bundle can acquire and utilize them. The main strength of OSGi is that the framework manages these bundles dynamically, allowing them to be upgraded without terminating the full application, as well as enabling the availability of the services to other bundles depending on the situation. That allows us providing new features and capabilities to the IoT Gateway by adding new services, which may use the services already existing in the framework, but keeping current features unaltered.

Using OSGi as development framework also eases development of the middleware layers, as we may focus on one single layer when developing, comprising one of more bundles, while the whole application layers will be arranged on execution time. Middle-layer interfaces are also defined to specify interoperability among adjacent layers and eliminate direct dependencies among bundles implementing each layer. According to Figure 8, the different layers have the following objectives.

- (i) The network bridge is a USB dongle with a ZigBee module that can be controlled through an AT command interface on a serial port. On the lower layer, the Serial Communication middle interface defines a SerialConnection service, which basically allows writing bytes and notifies about incoming bytes, and a SerialDriver service, which is in charge of creating and discovering available SerialConnection services. Main bundle implementing this layer operates the UART interface, but other stream-based interfaces, such as a Bluetooth connection, may adopt the same middle-layer interface, allowing communication with Bluetooth devices transparently to the upper layers. In our particular case, we have implemented an application service that wraps a SerialConnection into a TCP socket, and at the remote client, another bundle creates a SerialConnection services that allows communication with the SerialConnection services on the server side like a local one. This would allow any service on the Internet to remotely handle the serial port traffic, which is very useful for debugging or auditing deployed IoT systems.
- (ii) On the NoT Bridge Interpretation layer, a Zigbee-Gateway bundle looks for newly created SerialConnection services, checks if they correspond to the Zigbee USB dongle, and creates ZigbeeGateway services implementing the AT command protocol in such a case. Again, the ZigbeeGateway service is defined in the ZigbeeGateway middle interface, which isolates layers and allows using different versions of the USB dongle.
- (iii) Above that, there is a ZigbeeDriver, which uses the ZigbeeGateway to accomplish network management tasks, such as network creation or device enumeration, and a Driver Manager which uses the ZigbeeDriver to perform automatic maintenance tasks such as message route maintenance. It would be possible to aggregate these services into a single one but that will introduce complexity and hinder interoperability, whereas using separated services increases reliability and robustness as units of code are smaller and easier to test. This allows also deploying gateway facilities to accomplish transversal tasks, such as network monitoring, debug, maintenance, and commissioning, which may use limited parts of the Driver Layer. In the case of having other networks, the scheme is similar. The ZigbeeDriver will create ZigbeeNode services representing nodes in the network which allows sending and receiving messages to and from the physical device and provides Zigbee related properties such as its MAC address or its type.
- (iv) On the CTP Devices layer, a CTP Driver service will use the ZigbeeNode services to create CTP Device services representing the real devices available on the NoT, following the CTP definition. This layer isolates devices' technology and registers them attending to their nature in order to provide interoperability; a temperature sensor always provides temperature the

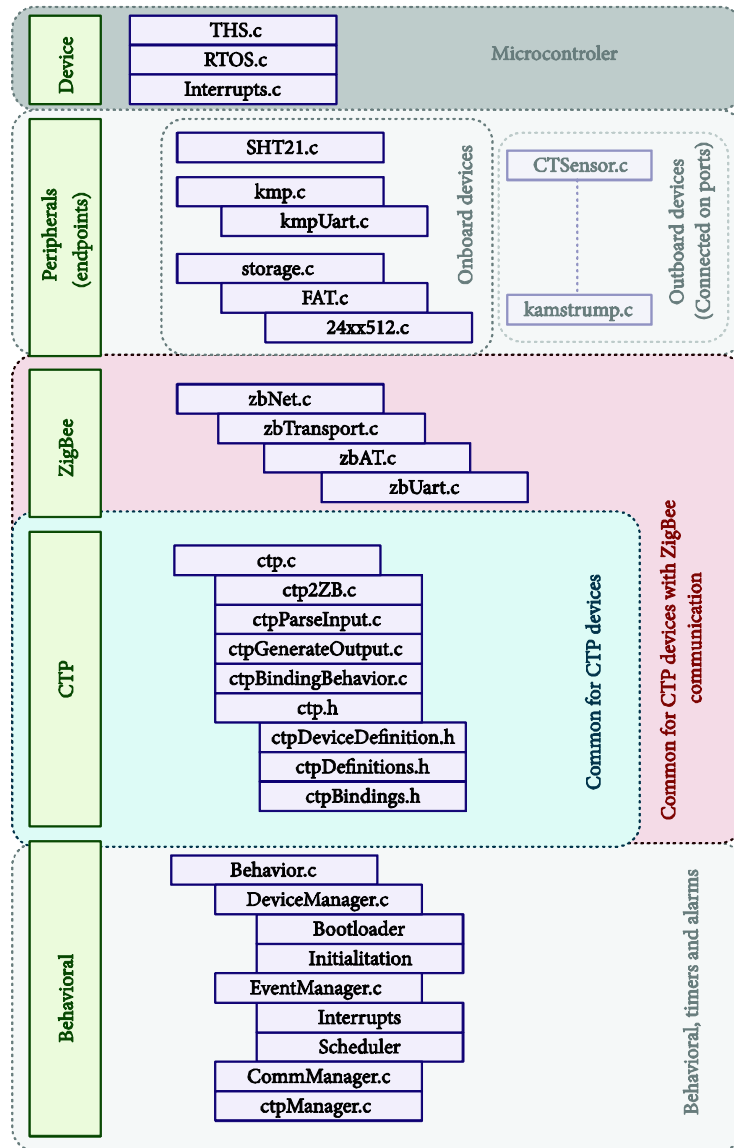


FIGURE 7: ZigBee thing firmware implementation.

same way regardless its technology. There are also different gateway facilities at this level (web services and TCP sockets) providing Internet access and virtual representation in order to allow remote applications to use NoT infrastructure.

- (v) At the IoT services layer, a Data Collector service tracks for CTP Device services of type Sensor, subscribes itself to receive a notification when a new sensor value is received, and sends a data report to a remote database, where it can be accessed from elsewhere.

At this point, local network devices, which were not able to reach the IoT by themselves, are now represented

by OSGi services which are smart enough to operate on the IoT and among them. Internet applications accessing those things require address resolution services which allow reaching them through an URL [2]. This is overcome by delegating things' addresses resolution to the IoT gateway which forwards incoming requests to the physical thing. Thus, accessing things from the Internet is granted by knowing the IoT gateway address. It is also feasible that things themselves access the IoT services directly; for example, we feed data from sensors to IoT services on the cloud specialized on data managing like Cosm [43] or Nimbis [44].

On top of the middleware described and thanks to the OSGi modularity, we also have developed communications terminal to sniff ZigBee communication (mainly intended as

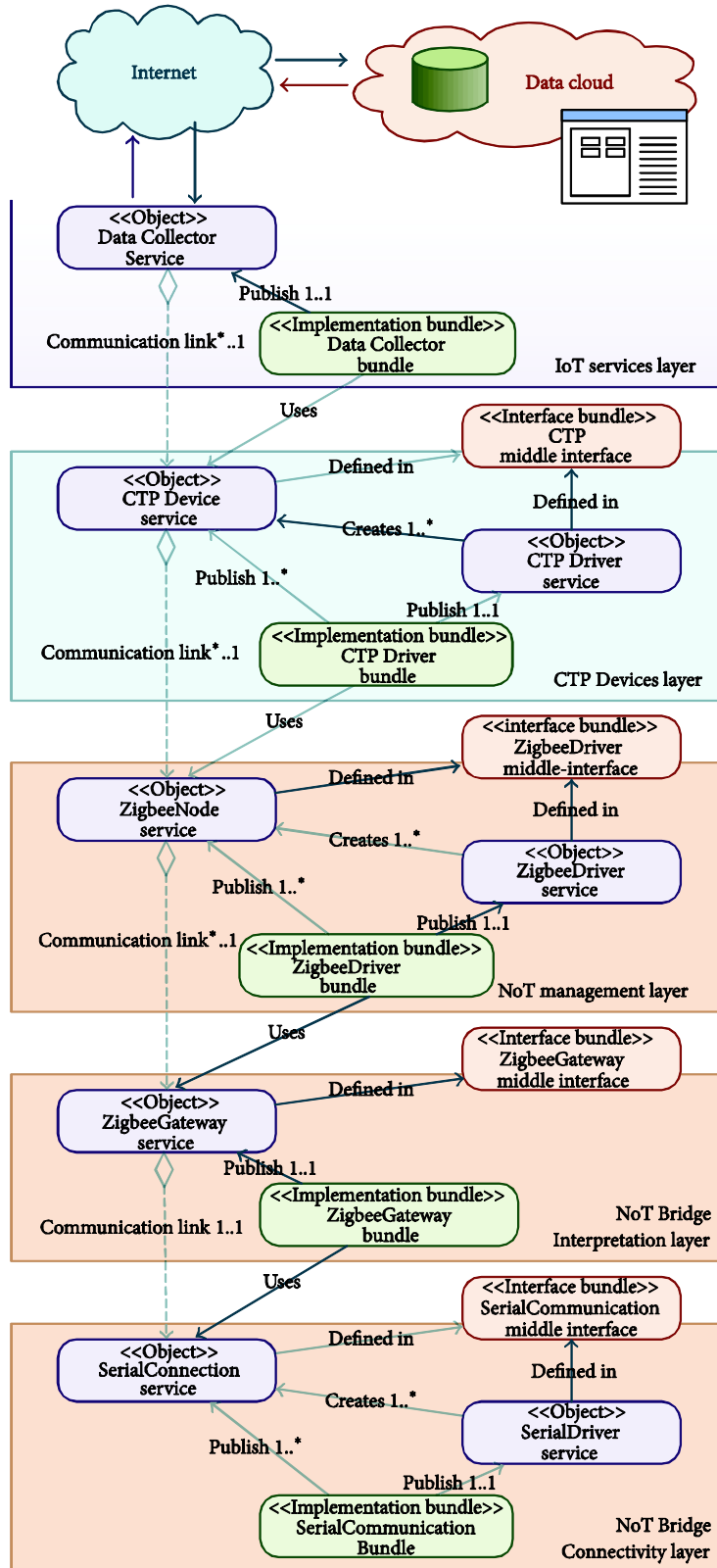


FIGURE 8: IoT gateway middleware architecture.

a development tool for hardware/firmware/software developers) and a Network Manager that allows full management and commissioning of deployed ZigBee networks.

5.4. System Performance. The system deployed is built by a backbone of 19 nodes (1 coordinator, 17 routers, and 1 data sink) that exchange network management messages. Also 90 sleepy sensors poll their parents every 10 seconds and report the data sink every 10 minutes. Due to network topology, some sensor messages must be relayed by routers up to five times to get to the data sink which passes them to the IoT gateway that maintains network's virtual image, checks data inconsistencies, registers loss of expected messages, and uploads data to exploitation database. These processes allow network commissioning, node-problem targeting, and data integrity validation.

Evaluating the quality of service (QoS) of an IoT application is not easy as it is a large and complex system based on heterogeneous technology and high application dependency. Currently, there are not well-defined standard metrics that can be used as a common agreed and widespread comparison of IoT systems; derived from this application specificity, researchers usually define their own metrics [45–47]. As IoT is usually made up by different subsystems, it is possible to analyze the layers separately; for example, there are many metrics to evaluate the effectiveness of data transfer in networks [48]; however, the success of an IoT should be assessed as a whole not just one particular aspect of the architecture [49].

The system proposed uses 90 sensors to deterministically measure ambient and power consumption information and make it available in the IoT. Three different areas are assessed: relative and absolute energetic cost, data efficiency, and message latency.

Data efficiency considers the amount of data generated in the ZigBee network and the data correctly stored in the cloud database. Similar indicators are used to assess the quality of a communication network, in which case it is common to consider lost messages and total messages. However, for the global evaluation of the IoT is preferable to consider both ends of the system, thus we use the messages generated by the physical *things* and the amount of data available in the logical scope. Note that if there would be nondeterministic events (e.g., alarms, presence detection, etc.) the data generated in the IoT will not be known a priori and also difficult to measure. We define the data efficiency of the IoT, DE_{IoT} , as

$$DE_{IoT} = \frac{DA_{IoT}}{DG_{NoT}} = \frac{DA_{IoT}}{\sum_{i=1}^n (MS_i \times ND_i)}, \quad (1)$$

where DA_{IoT} is the data available on the IoT, DG_{NoT} is the data generated by the NoT, n is the number of *things*, MS_i is the number of messages sent by *thing* I , and ND_i is the amount of data sent in each message (we assume this is constant for all the messages sent by a *thing*). This value can be measured accumulated or disaggregated in different periods to assess the variation of stability over the time. In our case, we check the number of new registers in database and considering that the total number of inputs should be 12960 per day

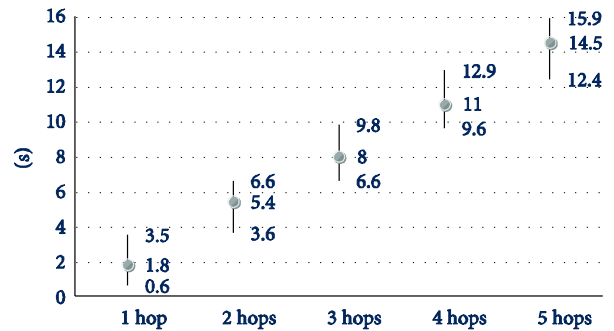


FIGURE 9: Latency time intervals.

(defined by the number of *things* and their scheduling), we can calculate the ratio. In our case, the accumulated data efficiency is 98.3%. It has been found that in general, errors are due to failures on the electrical supply or Ethernet network not directly attributable to the system.

Message latency quantifies the availability of a *thing* in order to exchange information with it. Again, we consider this availability from the IoT layer, that is, how much time takes to force a sensor to refresh, and effectively update the data in the cloud. There are two main factors that influence this indicator: how many hops away from the gateway is the sensor and how much time does the sensor spend in sleep mode (i.e., disconnected from the ZigBee network). Thus, we define the message latency per hop, MLH_j , as:

$$MLH_j = \frac{\sum_{i=1}^{n_j} RT_{ij}}{n_j}, \quad (2)$$

where RT_{ij} is the response time for *thing* i , which is j hops away from the gateway, and n_j is the number of *things* being j hops away from the gateway. Figure 9 shows the latency intervals (in seconds) within a 95% confidence interval according to the distance in hops between sensor and gateway. If we need to provide a global metric of the system latency we would say it will be between 0,6 s and 15,9 s.

Energy consumption of a device is a common indicator of its efficiency. In the particular case of IoT, we must take into consideration the consumption of the *things* and also communications infrastructure (routers) and logical infrastructure (gateway). Given the data volume managed, energy consumption of routers and gateway is independent from the amount of data sent by *things*, and the absolute energetic cost of the system over time $AEC(t)$ can be defined as follows:

$$AEC(t) = \left[P_{Gtw} + n_R \times P_R + \sum_{i=1}^n P_i \right] \times t, \quad (3)$$

where P_{Gtw} is the power consumption of the gateway, P_R is the power consumption of a router, n_R is the number of routers, P_i is the power consumption of *thing* i , and n is the number of *things*. As we show in [41] to calculate a *thing's* power consumption, a good characterization of its duty cycle is required. We have defined the figure of merit of power

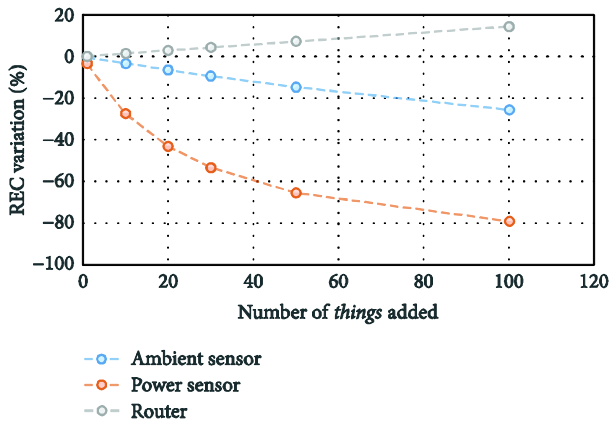


FIGURE 10: Relative energetic cost variation with respect to the proposed scenario when including new devices.

consumption for each type of *thing* and the routers and we consider constant the power consumption of the gateway. For the proposed IoT, the absolute energetic cost in one day is 19,76 MJ (5,49 kW·h). It is important to remark that only 0,013% of the energy is due to *things*, battery-powered devices. Given that in the proposed scenario, the number of data and time are directly related, we can also define the relative energetic cost REC as the energy required per byte of processed data during a day:

$$REC = \frac{AEC(t)}{DA_{IoT}} \Big|_{1 \text{ day}} \quad (4)$$

For the present IoT application we have a relative energetic cost of 121,97 J per byte sent. This includes 15 mJ corresponding to the energy drained from batteries. This parameter is related to the scalability of the network; if we enlarge the communications infrastructure (more routers to have broader coverage) and increase the number of *things* (to have more measurement points), relative energetic cost varies as in Figure 10.

Including new sensors supposes decreasing the REC as they provide additional data with reduced energy consumption. Specifically, power sensor consumption is related to a better REC than ambient sensor as it sends more data (44 bytes versus 4 bytes) with a similar energy consumption. As expected, including routers improves network backbone and/or range but worsens the metric, as they do not increase DA_{IoT} .

6. Discussion

Main conclusion of the described field trial is that architecture and the protocol proposed are feasible in large and long-term IoT deployments. Also it demonstrates that implementation of CTP over ZigBee in order to create low power *things* (running with batteries for a year) that efficiently integrates in an IoT system is possible. As we developed the whole system, from the hardware design of *things* to the service implementation, our concerns have been from the limited

resources of hardware and firmware to the versatility and generality required by applications.

In order to analyze under which circumstances CTP is a convenient option, Table 1 compares it with main IoT protocols mentioned in Section 2. Three different levels are identified: (1) standard communication protocols (6LowPAN, RFID, WiFi, Cellular, ZigBee, and Bluetooth), (2) protocols abstracting from communication media and being mounted over the protocol's payload (IEEE1451, CTP), and (3) protocols assuming IP connectivity on anything (CoAP, RESTfull-HTTP, XMPP, MQTT, SensorWeb, EEML, and SenseWeb). Comparison items are as follow.

- (i) Application layer interoperability among *things* indicates whether *things* can effectively exchange information among them, for example, if a light controller (protocol A) can be operated by a light sensor (protocol B). Communication standards (1) are limited on this because they are not intended to define how to interoperate with other standards. On the other side, protocols abstracting from communication standard (2, 3) are precisely designed to enable this feature. Also IP-based protocols (3) are more restrictive as they need that *things* are IP enabled.
- (ii) *Things'* representation models indicate if the protocol provides a virtual representation of *things*; for example, a temperature sensor has some characteristics (range, accuracy, etc.) and provides some methods (get temperature measurement, configure it, etc.). The protocols that just consider data exchange (e.g., 6LowPAN, WiFi, or MQTT) do not provide this definition hindering interoperability. ZigBee and Bluetooth define some *things*, those considered in their applications. IEEE1451, CTP, and SensorWeb define how anything needs to be specified, for example, the datasheet format.
- (iii) *Things'* interaction model: interaction means on step further than representation as it implies providing relationships among *things*, for example, how a light controller can be operated by a light sensor.
- (iv) Suitability for low power and lossy networks: this relies very much on the possibility to run on wireless sensor network standards, mainly ZigBee and 6Low-PAN.
- (v) Simplicity and exhaustiveness are important features that determine adoption of protocols. For example, IEEE1451 is a very exhaustive protocol defining everything in a sensor, but precisely this makes its use complicated by an app developer that just wants temperature value of a sensor.

According to Table 1, most similar protocols are CTP, IEEE1451, and ZigBee Cluster Library. In order to make a more detailed comparison among them, we define a scenario based on a ZigBee temperature sensor where these three specifications are encapsulated in the payload of the ZigBee application layer (Figure 11).

TABLE 1: IoT protocols comparison.

		Application layer interoperability among things	Things' representation models	Things' interaction model	LLN (Low Power and Lossy Networks) suitability	Simplicity	Exhaustiveness and level of detail
1	6lowPAN, RFID, WiFi, and Celular	Limited to standard (stack layer)	No	No	6lowPAN: excellent Others: fair	Not applicable (App. layer not defined)	Not applicable (App. layer not defined)
	ZigBee Cluster Library, Bluetooth Profiles	Limited to standard (App. layer)	Yes, but limited to specific applications	Yes, but limited to specific applications	ZigBee: excellent Bluetooth: fair	Good	Excellent
2	IEEE1451	Full (delegated to NoT protocol)	Yes, but limited to sensor and actuators	Yes, but limited to sensor and actuators	Excellent	Good	Excellent
	CTP	Full (delegated to NoT protocol)	Yes	Yes	Excellent	Excellent	Good
3	CoAP, RESTfullHTTP, XMPP, MQTT	Full (delegated to IP protocol)	No	No	CoAP: good (UDP) Others: fair (TCP)	Not applicable (App. layer not defined)	Not applicable (App. layer not defined)
	SensorWeb, EEML, SenseWeb	Full (delegated to IP protocol)	Yes	No	Fair (TCP)	EEML: Excellent Others: Fair	EEML: Good Others: Excellent

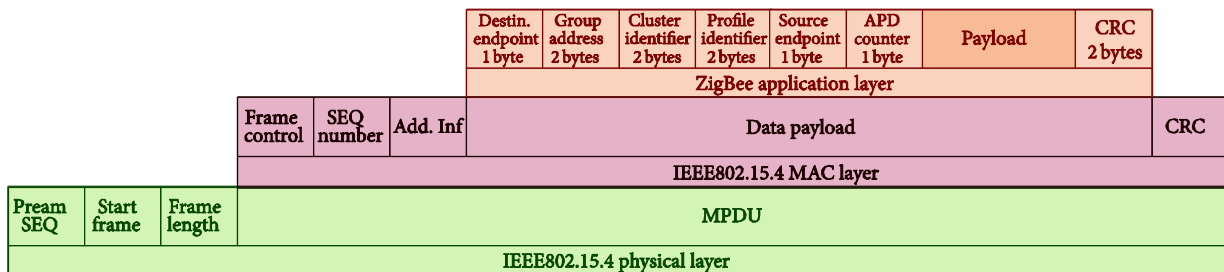


FIGURE 11: ZigBee protocol encapsulation.

Communication is established through requests and corresponding responses; Table 2 contains the frame descriptions for the three cases. Each frame includes different fields defined in the specifications.

In order to use the temperature sensor several requests need to be answered by the sensor: (1) retrieving general information about the device, (2) retrieving channel/endpoint mandatory information, and (3) retrieving temperature measurement. If using ZCL, sensor temperature must be 2 bytes in length, in degrees Celsius, and specified in the range from -273.15°C to 327.67°C with a resolution of 0.01°C . Thus, step 2 is not needed as information about the measure is already defined. This is positive in terms of easy use but limitative in some cases; if using CTP or IEEE 1451, variables such as accuracy, range, units, and so forth are open to the hardware developer and must be specified in the channel/endpoint mandatory information. Table 3 indicates the number of bytes exchanged for each

action and the number of variables encoded. It should be noted that just mandatory fields are considered in the table.

Regarding protocol efficiency, it is obvious that ZCL is the most efficient, but this has important implications: as ZCL focuses on specific application domains (home and building automation, health, etc.) if the *thing* is not specified in the standard or the representation of the information differs from it, its implementation is not possible and thus it will not be interoperable. For example, there is no way to use inertial sensors according to ZCL.

On the other hand, IEEE 1451 is the heaviest protocol because it leaves open a lot of variables. This flexibility turns to be its main drawback to be used in IoT applications because it makes it too complicated for developers not versed into electronics. Additionally, as it is more oriented to electronics than to application, it does not consider human-machine interfaces in its specification, just sensors and actuators.

TABLE 2: Frame description of IEEE 1451, CTP, and ZCL.

		Header	Payload
IEEE 1451	Request (6 + n) bytes	Destination transducer channel: 2 bytes Command Class: 1 byte Command Function: 1 byte Offset Length: 2 bytes	Data: n bytes
	Response (3 + n) bytes	Success flag: 1 byte Offset Length: 2 bytes	Data: n bytes
CTP	CTP Frame (5 + n) bytes	Endpoint destination: 1 byte Length: 2 bytes Cluster identification: 1 byte Command identifier: 1 byte	Data: n bytes
ZigBee Cluster Library	ZCL Frame (5 + n) bytes	Frame Control: 1 byte Manufacturer code: 2 bytes Transaction sequence number: 1 byte Command identifier: 1 byte	Id attribute: 2 bytes Value attribute: n bytes : : Id attribute m : 2 bytes Value attribute m : n bytes

TABLE 3: Number of payload bytes (differentiating request + response) and variables associated.

	IEEE 1451		CTP		ZigBee Cluster Library		Observations
	Bytes	Variables	Bytes	Variables	Bytes	Variables	
Retrieve general information about the device	50 (7 + 43) 42 (7 + 35)	21	45 (5 + 31)	5	14 (7 + 7)	1	In case of ZCL, information obtained is partial, same amount/type of variables must be done from a lower level of the protocol; at ZigBee Device Object.
Retrieve channel/endpoint mandatory information	111 (7 + 104) 33 (7 + 26)	18	34 (5 + 29)	7	—	—	ZCL strictly defines the nature of the variables in each cluster, so no need to declaration.
Retrieve temperature measurement	12 (7 + 5)	1	12 (5 + 7)	1	14 (7 + 7)	1	

As a summary, CTP is a balanced protocol especially suited for the IoT allowing definition of any device and just specifying those variables that are needed at application level. As it can be efficiently encapsulated in any communication protocol, it is strongly focused on the interoperability of *things* while considering their technical limitations (energy, processing, and communication capabilities). CTP is based on an ontological representation and interaction model; thus, besides interoperability, it allows local intelligence and interaction among *things*. Also as it describes the characteristics and properties of *things*, higher-level protocols can use it as a source of information.

7. Conclusions

IoT is perceived as a huge generator of services and applications, but it requires that two important issues to be solved: *things*' connectivity (communication of the physical *things* with the Internet) and interoperability at all levels (understanding of the information exchanged). This paper emphasizes the need to maintain an integrative and broad point of view when considering architectures and protocols for IoT. Considering IoT development areas and their

associated technologies, an architecture and protocol with a comprehensive view considering current technological capabilities at all levels (services, gateway communications, firmware, and hardware) are proposed.

In order to tackle connectivity challenge, the appropriateness of using gateway-based solutions to connect Networks of *Things* with the Internet has been discussed. This is considered an optimal way to solve the problem of the heterogeneous networks, jumping from the real world to the IP world and ensuring the unambiguous designation of each of the *things* in the Internet, performing a tunneling process (e.g., the need of a unique identification). Regarding the functionality of the IoT gateway, the use of layered and modular middleware architecture to constitute a versatile, interoperable, scalable, and easy to maintain system has been proposed.

Common *Things* Protocol (CTP) has been presented as a solution to provide interoperability among *things*. Main guidelines considered in its design are an ontological representation and interaction model of *things* and implementation feasibility in standard communication protocols. CTP reflects the need for equilibrium between the networks of *things*, data traffic, and virtualized world of *things*, which

is not common in the current proposals. Main principles of CTP are self-description of the nature and capabilities of the *thing*, organization capabilities through the endpoint and cluster concepts, simplifying the use of the *thing* in standard situations through mechanisms such as modes and scenarios, allowing distributed intelligence by using bindings and behaviors, and being simple and compact to ease its implementation fitting on current standard communication protocols.

The IoT architecture (ZigBee network of *things*, IoT gateway and related Internet services) and CTP proposal have been implemented in two European research projects related to smart environments for Ambient Assisted Living and energy efficiency. The paper describes specific hardware and software implementations and deployment in large scale environments, with real end users, during periods of several months. We also measure energetic cost, data efficiency, and message latency metrics demonstrating proposal's feasibility and suitability in order to meet current IoT requirements.

This paper does not intend to define a standard but an initial proposal to adopt a minimum agreement (currently not considered in the state of the art) with a global and inclusive vision that facilitates the development of the IoT. To this end, it should be mentioned that most of the developments shown have been carried out under open source license, in particular CTP is accessible and well documented [50].

Conflict of Interests

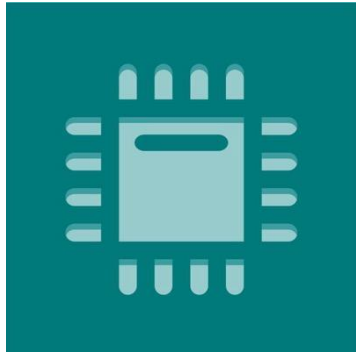
The authors declare that there is no conflict of interests regarding the publication of this paper.

References

- [1] I. T. Union, "ITU Internet Reports 2005: The Internet of *Things*," 2005.
- [2] L. Atzori, A. Iera, and G. Morabito, "The Internet of *Things*: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [3] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of *things*," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, 2010.
- [4] R. V. Kulkarni, A. Förster, and G. K. Venayagamoorthy, "Computational intelligence in wireless sensor networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 1, pp. 68–96, 2011.
- [5] ISTAG, "Orientations for EU ICT R&D & Innovation beyond 2013-10 keys recommendation," July 2011, http://cordis.europa.eu/fp7/ict/istag/documents/istag_key_recommendations_beyond_2013_full.pdf.
- [6] M. Swan, "Sensor Mania! The Internet of *Things*, Wearable Computing, Objective Metrics, and the Quantified Self 2. 0," *Journal of Sensor and Actuator Networks*, vol. 1, no. 3, pp. 217–253, 2012.
- [7] "sensei (Real World Dimension of the NETwork of the Future)," <http://www.ict-sensei.org/index.php>.
- [8] "IoT- A, (Internet of *Things* Architecture)," <http://www.iot-a.eu/public>.
- [9] "Internet of *Things* Strategic Research Roadmap," European Commission-Information Society and Media DG-BU31 01/18 B-1049, Brussels, Belgium, 2009.
- [10] D. Uckelmann, M. Harrison, and M. Florian, "An architectural approach towards the future internet of *things*," in *Architecting the Internet of Things*, pp. 1–24, Springer, 2011.
- [11] D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac, "Internet of *things*: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.
- [12] MQTT, <http://mqtt.org/>.
- [13] "ipSo Alliance," <http://www.ipso-alliance.org/>.
- [14] T. Usländer, A. Berre, C. Granell et al., "The future internet enablement of the environment information space," in *Proceedings of the International Symposium on Environmental Software Systems (ISESS '13)*, Neusiedl am See, Austria, 2013.
- [15] C. Gómez, J. Paradells, and J. Caballero, *Sensors Everywhere. Wireless Network Technologies and Solutions*, Fundación Vodafone España, 2010.
- [16] A. Kapadia, S. Myers, X. Wang, and G. Fox, "Secure cloud computing with brokered trusted sensor networks," in *Proceedings of the International Symposium on Collaborative Technologies and Systems (CTS '10)*, pp. 581–592, May 2010.
- [17] A. Ibarz, G. Bauer, R. Casas, A. Marco, and P. Lukowicz, "Design and evaluation of a sound based water flow measurement system," *Lecture Notes in Computer Science*, vol. 5279, pp. 41–54, 2008.
- [18] ZigBee Specification, "ZigBee Cluster Library Specification," (053474r17), 2008.
- [19] Y.-F. Lee, H.-S. Liu, M.-S. Wei, and C.-H. Peng, "A flexible binding mechanism for ZigBee sensors," in *Proceedings of the 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '09)*, pp. 273–278, December 2009.
- [20] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: an application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, vol. 16, no. 2, pp. 62–67, 2012.
- [21] XMPP Standards Foundation, "XMPP Standard," <http://xmpp.org/>.
- [22] "Constrained RESTful Environments (core)," <https://data-tracker.ietf.org/wg/core/charter/>.
- [23] "How Can IEEE, 1451 Be Applied," June 2007, <http://iee1451.nist.gov/>.
- [24] I. I. a. M. Society, *IEEE Standard for a Smart Transducer Interface for Sensors and Actuators*, 2007.
- [25] D. Sweetser, V. Sweetser, and J. Nemeth-Johannes, "A modular approach to IEEE-1451.5 wireless sensor development," in *Proceedings of the IEEE Sensors Applications Symposium*, pp. 82–87, February 2006.
- [26] J. Higuera, J. Polo, and M. Gasulla, "A ZigBee Wireless sensor network compliant with the IEEE 1451 standard," in *Proceedings of the IEEE Sensors Applications Symposium (SAS '09)*, pp. 309–313, February 2009.
- [27] J. E. Higuera and J. Polo, "IEEE 1451 standard in 6LoWPAN sensor networks using a compact physical-layer transducer electronic datasheet," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 8, pp. 2751–2758, 2011.
- [28] Z. Wemlinger and L. Holder, "The COSE ontology: bringing the semantic web to smart environments," in *Toward Useful Services for Elderly and People with Disabilities*, vol. 6719, pp. 205–209, Springer, 2011.
- [29] D. Bonino, E. Castellina, and F. Corno, "DOG: an ontology-powered OSGi domotic gateway," in *Proceedings of the 20th IEEE International Conference on Tools with Artificial Intelligence (ICTAI '08)*, pp. 157–160, November 2008.

- [30] W. Wang, S. De, G. Cassar, and K. Moessner, "Knowledge representation in the internet of things: semantic modelling and its applications," *Automatika*, vol. 54, no. 4, pp. 388–400, 2013.
- [31] B. Christophe, "Semantic profiles to model the 'web of things,'" in *Proceedings of the 7th International Conference on Semantics, Knowledge, and Grids (SKG '11)*, pp. 51–58, October 2011.
- [32] E. Y. Song and K. Lee, "Understanding IEEE 1451—networked smart transducer interface standard—what is a smart transducer?" *IEEE Instrumentation and Measurement Magazine*, vol. 11, no. 2, pp. 11–17, 2008.
- [33] R. Johnson and S. P. Woods, "Proposed enhancements to the IEEE, 1451. 2 standard for smart transducers," September 2009, <http://archives.sensormag.com/articles/0901/74/main.shtml>.
- [34] M. Compton, P. Barnaghi, L. Bermudez et al., "The SSN ontology of the W3C semantic sensor network incubator group," *Web Semantics*, vol. 17, pp. 25–32, 2012.
- [35] L. Feng, P. M. G. Apers, and W. Jonker, "Towards context-aware data management for ambient intelligence," in *Database and Expert Systems Applications*, vol. 3180 of *Lecture Notes in Computer Science*, pp. 422–431, Springer, 2004.
- [36] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: the format war hits the factory floor," *IEEE Industrial Electronics Magazine*, vol. 5, no. 4, pp. 23–34, 2011.
- [37] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.
- [38] European 6th Framework Programme for Research and Technological Development, "Easy Line Plus," <http://www.easylines-plus.com/>.
- [39] C. P. E. Commision, "Renaissance," <http://www.renaissance-project.eu/?lang=en>.
- [40] U. o. Zaragoza, "Liga Energetica edificio I+D+i," <http://proyectosostenibilidad.unizar.es/institutos/index.php/monitorizacion>.
- [41] Á. Asensio, R. Blasco, Á. Marco, and R. Casas, "Hardware architecture design for WSN runtime extension," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 136745, 11 pages, 2013.
- [42] O. A. website, "OSGi Alliance website," <http://www.osgi.org/Main/HomePage>.
- [43] <http://www.cosm.com>.
- [44] <http://www.nimbits.com>.
- [45] M. W. Ryu, J. Kim, S. S. Lee, and M. H. Song, "Survey on internet of things: toward case study," *Smart Computing Review*, vol. 2, no. 3, 2012.
- [46] M. Paschou, E. Sakkopoulos, E. Sourla, and A. Tsakalidis, "Health Internet of Things: metrics and methods for efficient data transfer," *Simulation Modelling Practice and Theory*, vol. 34, pp. 186–199, 2013.
- [47] A. P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, and M. Zorzi, "Architecture and protocols for the internet of things: a case study," in *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM '10)*, pp. 678–683, April 2010.
- [48] S. Forsström, P. Österberg, and T. Kanter, "Evaluating ubiquitous sensor information sharing on the internet of things," in *Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012.
- [49] J. Gubbia, R. Buyyab, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer Systems*, no. 29, pp. 1645–1660, 2013.
- [50] HOWLab, 2013, <http://openlab.unizar.es/index.php/conocimiento/ctp>.

2.4 MANAGING EMERGENCY SITUATIONS IN THE SMART CITY: THE SMART SIGNAL



Ángel Asensio, Teresa Blanco, Rubén Blasco, Álvaro Marco, Roberto Casas
Sensors
doi:10.3390/s150614370.

2015

RESUMEN:

En este trabajo, en base a los modelos expuestos en el “Manuscrito 3 (Interoperabilidad)” se ha abordado el reto de convertir un objeto sin tecnología asociada (en este caso una señal) en una Cosa de la IoT para dar servicio a la Smart City, surgiendo de este modo un nuevo elemento: la *Smart Signal*. Esta investigación ha estado articulada en torno a diversos proyectos con la empresa Implaser, en los que desde el principio se consideró el potencial de IoT para encontrar la solución requerida. Los resultados descritos en este trabajo han constituido la base tecnológica sobre la que se asienta una de las patentes (“Intelligent system for signaling an emergency in tunnels”) realizadas en el ámbito de esta tesis.

Se expone el desarrollo del sistema de señalización inteligente abarcando desde la señal en sí misma, hasta la arquitectura. Las propuestas de CTP de “Manuscrito 3 (Interoperabilidad)” se han aplicado a este nuevo caso práctico y tomando como base las consideraciones de “Manuscrito 1 (Eficiencia HW)” se proponen estrategias diferentes para mejorar la eficiencia energética de una Cosa. Para lo cual no solo se considera como un dispositivo electrónico, sino que en el modelo se integran otras fuentes de energía y mecanismos de almacenamiento de energía. Se aborda el despliegue de un demostrador del sistema en el túnel de Monrepós, para lo que se hace uso de una serie de herramientas de despliegue que facilitan el trabajo. De igual modo las métricas anteriormente expuestas, pasan a ser aplicadas como una herramienta de autoevaluación del funcionamiento del sistema. Los resultados de este trabajo constituyen la base sobre la que se va a desarrollar el proyecto SigueTu, actualmente en curso.

Article

Managing Emergency Situations in the Smart City: The Smart Signal

Ángel Asensio *, Teresa Blanco, Rubén Blasco, Álvaro Marco and Roberto Casas

Aragón Institute of Engineering Research (I3A), Universidad Zaragoza, Edificio IDI, Mariano Esquillor s/n, Zaragoza 50018, Spain; E-Mails: ter@unizar.es (T.B.); rblasco@unizar.es (R.B.); amarco@unizar.es (Á.M.); rcasas@unizar.es (R.C.)

* Author to whom correspondence should be addressed; E-Mail: aasensio@unizar.es; Tel.: +34-876-555-464.

Academic Editors: Antonio Puliafito, Symeon Papavassiliou and Dario Bruneo

Received: 30 April 2015 / Accepted: 8 June 2015 / Published: 18 June 2015

Abstract: In a city there are numerous items, many of them unnoticed but essential; this is the case of the signals. Signals are considered objects with reduced technological interest, but in this paper we prove that making them smart and integrating in the IoT (Internet of Things) could be a relevant contribution to the Smart City. This paper presents the concept of Smart Signal, as a device conscious of its context, with communication skills, able to offer the best message to the user, and as a ubiquitous element that contributes with information to the city. We present the design considerations and a real implementation and validation of the system in one of the most challenging environments that may exist in a city: a tunnel. The main advantages of the *Smart Signal* are the improvement of the actual functionality of the signal providing new interaction capabilities with users and a new sensory mechanism of the Smart City.

Keywords: *Smart Signal*; Smart City; wireless networks; tunnel

1. Introduction

A signal is a visual representation that transmits particular information in a quick and intuitive way. Signals should be designed to rapidly capture the attention of people, being their iconography easily understandable and self-contained, in order to ensure that the message is immediately read without any

misinterpretation. Usually signals transmit data related to the context in which they are located and offer information about how to interact with them. In some types of signaling, such as emergency signals, the transmitted information is critical, as it warns about potential risks or gives vital cautions about how to proceed to face or to avoid these risks. That is why signals are more common and necessary in complex or hostile environments, which should be approached with particular caution. Nonetheless, in these contexts, signaling systems are limited nowadays: most of them are constituted either by merely passive elements that keep their message always visible, or by some kind of lighting controlled by simple external events [1,2] (as the ambient light level, alarm systems, *etc.*).

Signaling systems are closely related to the cities, either to the infrastructure of the city itself, to the buildings and facilities that the city contains, or to the communication channels within the city.

Together with the signaling systems, other typical systems on cities are those intended to light the streets or public spaces. Both share characteristics, because they are composed of a lot of devices scattered throughout the entire city, *a priori*, and are simple devices of which the citizens are not aware. Unlike lighting systems, which have seen increases in their performances and efficiency using new technologies [3,4], the same has not happened with signaling systems. So, one of the aims of this paper is to show the possibilities that arise when performing a similar process in the field of signaling.

Currently, new capabilities are being included to the basic model of signal. Thus, in the area of context awareness, innovation is mainly focused on traffic control systems [5,6] (even commercial solutions [7]) and context awareness signaling in hostile environments [8–10]. The user interaction is evolving through variable message panels, whose usefulness has been demonstrated, although some doubts about the induction of distractions on drivers have arisen [11].

From the perspective of ICT (Information and Communications Technologies), it is common to use the term Smart City [12] to refer to the “city of the future” [13]. The current development of smart cities is in the early stages [14,15]; most of the services currently developed, are based on monitoring or sensing variables to extract information, analyze and show it to the user in a more useful way. This applies to numerous scopes like traffic management, monitoring of pollution [16] and environmental variables, water supply analysis [17], public WiFi, citizen information services based on position, or systems for the preservation of historical heritage [18]. To a lesser extent, it is possible to find examples of control of some of the typical systems of a city such as street lighting systems [19], traffic management and even power management [20] (integrating the Smart Grid inside the Smart City). There are many lines of work around the concept of Smart City and it is expected to become a sizable market, with projections of nearly \$40 billion spent on smart-cities technologies by 2016.

The concept of Smart City has a strong technological component as it is built by interrelated environments in which different embedded elements are able to interact among them, and with users who inhabit them, in order to generate new services. The so-called Internet of Things (IoT) is shown as one of its basic components, since it proposes that everyday objects are globally accessible from the Internet and integrated into new services (Internet of Services (IoS)), having a remarkable impact in our society. Next decade will be dedicated to the Future Internet that, with its components IoS and [21] IoT, will promote the development of the concept of Smart City.

Since an intelligent signaling system must necessarily be integrated into its environment; in the context of Smart City, such systems should be able to interact with those related to city management. From a technical perspective, it is necessary that the new *Smart Signal* is one of the things that will be part of the

IoT. As in many other cases, incorporating a system into the Smart City, or a device into the Internet of Things, nowadays, is done by adding some ICTs (mainly communications, sensors or processing) to the original element. In this way, a *Smart Signal* will most be a traditional “signal”, to which some “smart” capabilities will be added.

When designing a signal, it is necessary also to analyze graphics design, semiotics, behavioral psychology of different people interactions with the user, *etc.* Much of these aspects have been overlooked in this paper, because they are away from the topic, but have been taken into account (thanks to the collaboration with the signaling company Implaser) when designing a concrete application.

Unlike other examples of systems that are evolving to be “smart”, the same trend is not seen in signals. This is because in any signaling system, the number of items is high and they are required to have a minimal cost. On the other hand, a signal is something that goes unnoticed due to its message often being very simple, but these messages are usually very important, and at some time critical. Thanks to technological advances (miniaturization, economic cost and energy consumption requirements), and the current trends on smart things, the Smart Signal will be completely viable. The transition from a signal to a Smart Signal evolves through several states in each of the following aspects:

- Message: From *static* (always visible the same message), to *active* (its visibility is controllable through blinking, fading, *etc.*), and finally *adaptive* (one message or another according to different circumstances).
- Control: From *uncontrollable*, to *controllable* (it is possible to define the behavior of the signal externally), and finally *autonomous* (the signal has the capability of control itself).
- Communications: From *isolated* (the signal has no communications capabilities), to *point to point* (the signal can communicate with a control point), and finally *mesh* (the signal can communicate with any of the elements on its surroundings).
- Context: From *isolate* (the signal has no knowledge about its environment), to *context awareness* (the signal has full knowledge about its environment, and can accommodate to it).
- Energetic dependence: From *external dependence* (the signal must constantly maintain power), to *autonomous* (for a while), and finally *self-sufficiency* (the signal does not need any external energy support).

A true Smart Signal must be aware of its context, able to analyze the situation and to inform optimally at all times. It must have communication skills that enable its integration into the IoT and share information and interact with other signals, thereby forming a network of intelligent signaling. The displayed message should be manageable both from a local intelligence (each signal decides its own message), from a network intelligence (depending on the state of the environment that spans the signaling system and on other messages from each signal) or even from external signaling network commands. The advantages of an intelligent signal against the current signs are:

- Improvement on the messages sent to users (who will have more and better capacity for effective decision-making).
- Messages are adapted to the circumstances of each moment.
- Interaction with new recipients of information (e.g., vehicles on a road), which will automate the sending of information, and facilitate certain actions (such as driving).

- Providing lots of geographically distributed information to other systems in real time, enhancing their capacity for analysis, forecasting of situations and incidents management.
- Increased possibilities for control signaling systems from both internal sensors and from external systems.

In this article, the concept of *Smart Signal* is presented and Section 2 deepens in the design of each of its components, the desirable characteristics and associated implications. *Smart Signal* concept is not addressed, as a single element, but as a multi-agent system, which forms intelligent signaling systems able to interoperate within larger entities, such as the Smart City. From this conceptualization, Section 3 presents the architecture and implementation of an intelligent system. The concept of *Smart Signal* is generic and can have different applications, as there exists different kinds of signals. This paper presents an example using Smart Signals within a smart emergency signaling system for tunnels and large infrastructures. Finally, in Section 4, we present the tests in laboratory and field and the results associated.

2. Smart Signal Design Consideration

According to state of the art, *Smart Things* are composed of different building blocks [22]. Figure 1 shows how this concept is particularized to the smart signal concept.

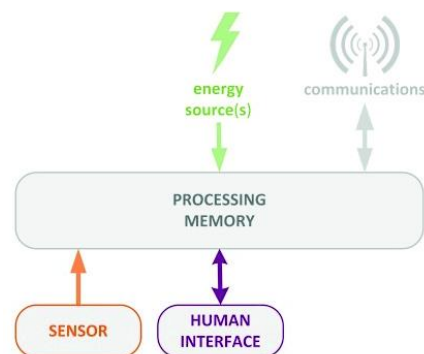


Figure 1. Smart Signal architecture.

The processor is the core of the *Smart Things* devoted to making decisions, managing energy and communications, providing intelligence, providing context awareness, *etc.* The memory is a resource for the processor on which information is stored (settings, measured values, *etc.*). The following subsections detail each of the surrounding blocks that provide the Smart Signal's functionality.

2.1. Human Interaction

Communication with users constitutes the main functionality of a signal. It must transmit to the people the message that the signal is intended for (for example, which direction to go in an emergency situation). Furthermore, smart signaling would aim to achieve a real human interaction, for example by getting user feedback (e.g., panic button in meeting point signal).

Human interaction in smart signaling has to overcome a difficult environment that demands immediacy and effectiveness on a close to instantaneous basis. Simple and direct messages are mandatory, so that mainly elementary (but commonly used) output interfaces (lights, beeps, *etc.*) should be usually considered.

Of course, the user must get the message meaning quickly and without any doubt, and appropriately decide the correct action, getting over a number of problematic situations in real environments, such as (i) a context with overwhelming information and stimuli; (ii) an unknown and stressful situation that sometimes even carries death risk; and (iii) an environment with communication blockings or interferences (for example, bad visibility of signals due to absence of electricity, hard to hear messages, difficulty to concentrate due to loud noise, *etc.*)

A smart signal will be aware of its context, it will have external connectivity and intelligence to decide how to handle its user interfaces to get user attention and to transmit the appropriate message. The basic steps of human-signal interaction are: capture the attention, inspection, exchange of information, information processing, and decision-making. Considering them, along with the previous technical demands, here are the essential Smart Signal human-machine interface elements:

- Simple optical markers: Points or bright surfaces, both continuous and time-varying (blinking, flashing, strobe) with bounded chromatic variety (possibility of various colors, but without frequent changes).
- Simple panel displays with simple variables messages, and scarcely changing over time.
- Simple hearing devices able to synthesize voice or just sirens-like.

2.2. Context Awareness

A *Smart Thing* achieves context awareness through its sensors, which are intended to get information about the surrounding context (e.g., if close fire exists, if there are people around, *etc.*). This information can be used to rule the signal's operation, to learn about the environment or just to report to a central management point. Sometimes, when we are interested in a magnitude inherent to the environment, a simple sensor can be used to measure it. In other cases, the *Smart Thing* must process the information of simple sensors (e.g., microphone) in real time in order to obtain higher level information (e.g., occupancy of a space through the analysis of the sound level monitored by a microphone). Therefore, it is relevant to identify what information from the context is required by a *Smart Thing*, which, obviously, will depend on its purpose. Focusing on the signals context, here we can see some of the variables that are susceptible to be measured, clustered by functionalities:

- Signals related with the ambient conditions. These kinds of signals measure one or more physical parameters of the environment and act according their value (e.g., a signal that monitors the temperature, “notifying about frost”, is enabled below T_{Low} and disabled over T_{High}). These are the most usual parameters:
 - Temperature, humidity and pressure: They are used to notify about changes in the environmental conditions that may affect the road safety.
 - Wind: It can be used to notify the user about crosswind or other dangerous situations due to the wind.
 - Light/luminosity: A *Smart Signal* using this sensor can adjust its illumination level depending of the ambient light.
 - Volatile Organic Compound (VOC): It is used to determine the environmental pollution.

- Signals related with the detection of atypical environmental situations. These kinds of signals monitor atypical and dangerous situations (that should never happen in a normal situations), notifying to a central management point and/or acting, e.g., changing a traffic light, lowering a barrier, *etc.* Most usual parameters are water (to detect flooding), radiation, smoke or VOC (in order to notify that a security threshold has been overpassed), *etc.*
- User interaction signals. These kinds of signals notify users about their actions (e.g., speeding on a road, turning on the lights in a tunnel, *etc.*). Usually, the signal is inactive and, when a user action is detected, it starts showing an indication during a predefined time (t_{Hold}), after which, the signal returns to the inactive state. In some cases, the signal can be disabled for new detections for a time (t_{Death}) in order to avoid multiple activations). The most usual parameters for this kind of signal are speed, presence/movement, proximity, light/luminosity, zone trespassing (for example by crossing an IR barrier), *etc.*

All these parameters could be measured by simple sensors. Though, it is possible to find signals that need more advanced/abstract information, e.g., to detect a fire (by merging information from smoke, temperature and VOC sensors) or to identify a person on the road (by using cameras and artificial intelligence algorithms).

2.3. Communications

Today, the advances in wireless communication and batteries allows for distributing small devices with different degrees of intelligence in the context, so smart environments are used more and more [23], and it is possible to find applications in many different scenarios, such as the city [24], home [25] or country [26], and even, in signalization applications, such as the traffic management [27]. In all these fields, communications between the elements of the system are fundamental.

Communication implies not only the capacity to exchange data, but also implies understanding the information codified inside them. All the communication protocols ensure physical communication between things in the same network if sharing the same protocol; nevertheless, if the application layer is not defined, things will not be understood among them unless previously agreed between developers. So, once efficient connectivity between devices is granted, we can define standards (based on semantics and ontologies for complex information processing and support higher levels of abstraction) that provide interpretation to data exchanged between integrated sensors and actuators and the virtual world [28].

Each scenario has its own communication requirements (amount of exchange data, frequency of communication, existed or accessible infrastructure, number of devices, *etc.*) that determinate the selection of a specific protocol out of a set of protocols. We can find several wired (X10, CAN, Ethernet, Modbus, Profibus, *etc.*) and wireless [29] (Bluetooth, ZigBee, WiFi, GSM, *etc.*) standard protocols that facilitate interoperability between systems.

In the case of a *Smart Signal*, the typical application scenario could have an elevated number of elements (from a few tens to hundreds), separated (between tens to hundreds of meters) and heterogeneously distributed within a large scenario, such as a city. Although the loss of one of the elements of the system is not usually critical, it is unacceptable that this loss implies a segmentation of the communications of the system. Therefore, a mesh topology able to define alternative routes when an unforeseen event happens is an adequate solution. Regarding these scenario requirements, a WSAAN (Wireless Sensor and Actuator

Network) appears to be a suitable solution for the communication between the distributed elements. This situation produces coexistence between wirelesses and wired protocols because the WSAN usually ends with the interconnection to a fixed infrastructure (Internet) based on IP (Internet Protocol) [30]. Currently, technologies based on IEEE802.15.4, 6LoWPAN and IPv6 are combining to meet this demand [31,32].

2.4. Energy

All devices need energy to operate, and it can come from the mains, from batteries or harvested from the environment. Signals often have to operate in environments where it is not advisable to perform a wired installation, so energy efficiency becomes a key aspect in design. Therefore, when performing the electronic design of a *Smart Signal*, it will be critical to take into consideration different strategies of low power design [33–37].

Obtaining energy from the environment, or energy harvesting [38], is the process by which energy from a source environment is collected, processed and stored for future use by a standalone system [39]. Some new street lighting systems and beacon lighting systems, which are being developed for the Smart City, are beginning to incorporate these capabilities [40]. The most likely energy sources to be used in the field of signaling are light (either sunlight outdoors [41], or artificial light indoors [42,43]), heat, micro wind generators [44,45], movements generated by traffic [46] or systems that leverage weight [47,48] (surface pressure over devices on the floor) of vehicle pressure systems. Combining these sources of energy with secondary batteries is usually a suitable appropriate solution.

In any case, power consumption of a *Smart Signal* will be a key factor to ensure its functionality; main sources of energy consumption are due to:

- Consumption associated with losses due to energy management (voltage conditioning, storage losses, etc.): E_{Lost} .
- Consumption associated with maintaining smart functionality (communication, sensing, data processing, etc.): $E_{SmartThing}$.
- Consumption associated with signaling: $E_{Signalling}$.

$$E_{Total} = E_{Lost} + E_{SmartThing} + E_{Signalling} \quad (1)$$

To implement its functionality, after an initialization stage, the *Smart Signal* executes repetitively the same cycle, switching between active and sleep states (Figure 2). The standard cycle of a *Smart Thing* will be similar to a WSN node, and each of its states has an associated power consumption (E_{state_n}):

- Sleep (E_{SLEEP}): This state is left, periodically or when an external event happens; the main causes for wake up are:
 - To stay (poll) or re-join the network, which runs every $T_{NETWORK}$.
 - To sense context, which runs every T_{SENSE} .
 - To refresh the status of the signal, which runs every T_{SIGNAL} .
 - Additionally, there may exist other causes, such as external events, that awake the system.
- Manage network status ($E_{NETWORK}$).
- Sense (E_{SENSE}): To get context awareness.

- Report Data ($E_{COMM DATA}$): To send collected data (each interval of time T_{REPORT} that could be greater than T_{SENSE}), if applicable.
- Process ($E_{PROCESS}$): To analyze data, execute commands, set signal status, etc.
- Report Status ($E_{COMM STATUS}$): To send, if applicable, new status of the signal.

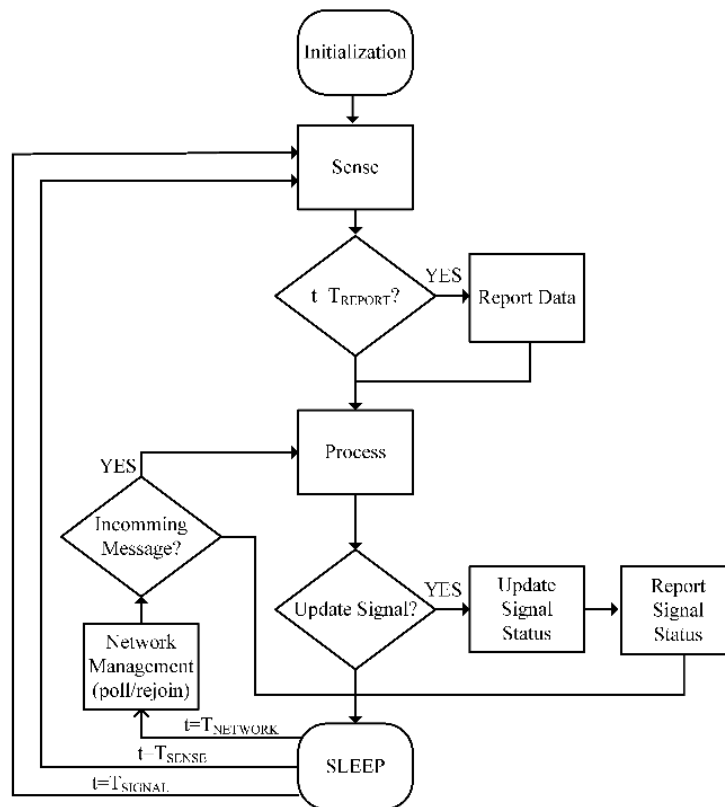


Figure 2. Operation cycle of Smart Signal.

The succession of these states, of predetermined time duration, is cyclically repeated, and defines the total $E_{SmartThing}$. This analysis is widely detailed in numerous papers, from which they can abstract the following considerations applied to *Smart Signal*:

- Consumption is periodic, with low average power consumption (in the order of the μW) that will mainly depend on the rate of time asleep/active.
- The higher peaks of power consumption (0.3 W–1 W) coincide with moments of communication.
- The need for keeping contact with the signal (to remain in the network) defines the $T_{NETWORK}$ time; periodically, the node will poll its parent asking for messages hold, and eventually will rejoin the network if the connection has been lost.

In short, the key to achieving low power consumption is to remain in a low power state most of the time.

Moreover, considering the activation time of the signal, the following classification of its consumption, $E_{Signalling}$, is possible:

- Constant: The signaling is active all the time but the message can change according to circumstances and/or external references (as for signals that show environment conditions).

- Cyclic: Periods of activity and inactivity are alternated (as for beacon signals that operate only at night).
- Punctual: The signaling is activated only under special circumstances (as for a fire emergency signaling in a building).

Overall, while in the activation period, the consumption will be continuous with a higher mean average power (order of tens of W) than in the previous case. It is possible to use advanced strategies to modulate the power consumption while the activation period (an example is exposed later in this paper), in order to improve energy efficiency.

So:

$$E_{SmartSignal} = E_{Initialization_SmartThing} + N_{cycles} \times E_{Cycle_SmartThing} + E_{Signalling} \quad (2)$$

$$\simeq t_{total}((1 - D_{ST}) \times E_{SLEEP} + D_{ST} \times E_{ACTIVE} + D_S \times E_{Signalling})$$

With:

$$D_{ST} = \frac{t_{cycle_SmartThing} - t_{sleep_SmartThing}}{t_{cycle_SmartThing}} \quad (3)$$

$$D_S = \frac{t_{on_Signal}}{t_{total}} \quad (4)$$

The issue of energy efficiency in a *Smart Signal* should be analyzed for each type of signal specifically, taking into account the environment in which it will be and the expected use. Given the dual nature of power consumption in a *Smart Signal*, it may be advisable to use two different energy sources for each of them, mainly to ease greater efficiency, but also for other reasons such as simplicity of the system, and cost. So, for example:

- For signals with few activations ($D_s \downarrow$), it may use a separate primary battery to operate the “*signal*”, and use another strategy (the same or another battery, energy harvesting, *etc.*) to power the “*Smart Thing*”.
- If the activation signal is continuous ($D_s \uparrow$), it is not feasible to use batteries primarily, but rather it is necessary to use a fixed power source ($E_{Signalling} \gg E_{SmartThing}$), whereas if the consumption related to the signal only is not excessive ($E_{Signalling} \times D_s \downarrow$), using energy harvesting strategies for the entire system can be considered.

3. Smart Signal System Implementation

In order to demonstrate the capabilities of the proposed *Smart Signal*, this concept has been applied to emergency signaling, considering its use in a particularly complex scenario, such as tunnels or corridors inside buildings. Current systems have important limitations: they are closed and static, and they just passively inform the user about the nearest safety point. Therefore, we have designed a smart signaling system, in which the signals have mechanisms to transmit the message clearly and efficiently to users, adapted to both the circumstances of the signal environment and the reminder signals’ visualizations. The goal is to guide people through the most effective route and avoid particularly dangerous situation unlike traditional signaling: leading to exits that are compromised and dangerous. In the case depicted in Figure 3, the emergency (a fire and smoke) has compromised one of the emergency exits. Therefore,

indications provided by some of the classic signals are unsafe, whereas the smart signals take this into account, and provide a safer indication.

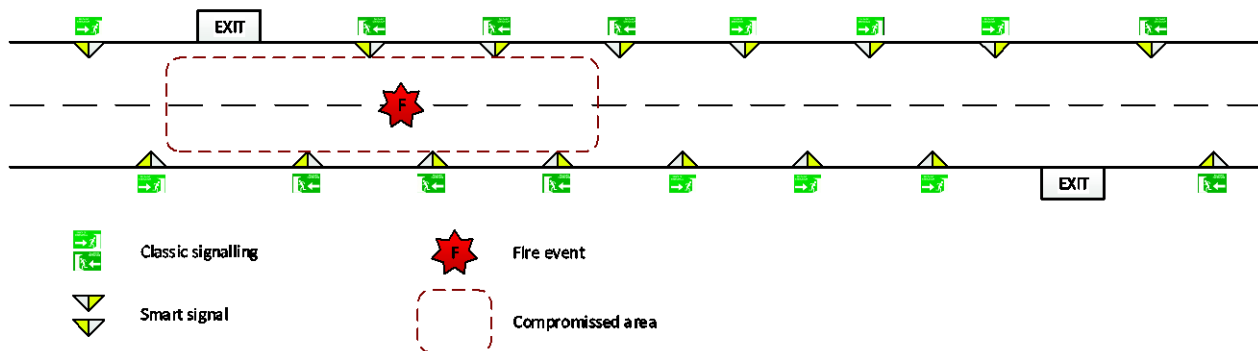


Figure 3. *Smart Signal* concept applied to emergency signaling in tunnels. The Smart Signals provide indications adapted to the emergency characteristics.

The Smart Signals will be able to gather information from their nearby environment and to report it regularly, and it is also required that they integrate with the in-place management and control systems that monitor, control and manage the equipment already installed in the tunnel. The latter is achieved by means of an OSGi (Open Services Gateway Initiative)-based [49] gateway, which acts as entry point for the *Smart Signals* network, and also allows providing specific services, such as system management or information processing.

3.1. Smart Signal

The development of a Smart Signal can be addressed as if it were a node of a WSN; this approach could simplify the process due to the know-how that already exists about them. Next, it will be exposed to the design of a *Smart Signal*, emphasizing the electronic design and user interaction.

3.1.1. User Interaction

When considering the design of the proposed signal, the main specification was clear: to guide the people inside the tunnel to the closest and safest exit, the fastest way as possible. When an emergency situation occurs, different phases need to take place to solve it [50]: (i) detection, characterized by the time elapsing since the emergency happens to the moment the alarm is triggered; (ii) alarm, characterized by the time that takes all the warnings to be active; (iii) response, characterized by the time taken by the people to acknowledge the alarm and reaction to it; and (iv) movement, as the time needed to make it to safety. Signals play a key role in the third and fourth stages, as users should use them to orientate and evacuate themselves. A person needs to create a mental egocentric sequential map to follow; in this regard, signals can be essential way-finding beacons that must quickly help him/her to decide which direction to take, and then, as he/she advances, confirm whether or not his/her decision is correct [51].

In the specific case of a fire in a tunnel, the scenario becomes extreme; for this reason, emergency signaling has the function of directing pedestrians quickly to the nearest emergency exit. There is evidence (from previous accidents and simulations) that in emergency situations there is a percentage of people with a high reluctance to abandon their vehicles, which results in fatal outcomes for them, so they should be

encouraged to leave the car for escape. The enormous burden of stress and bewilderment the user experiences in an event like this, which dramatically affects the ability to make clear decisions, is worsened by the existence of smoke. Apart from being an agent of intoxication, it makes the user become blind, thus, it is an important cause of confusion and disorientation. The evacuation phases (response and movement) are absolutely critical: signaling has to attract the user to the wall in order to offer him/her a benchmark; then, it has to transmit the information in a simple, direct, and effective way that is any free of dual meaning; and finally, it has to confidently make the user follow the safest way without delay or doubts. In summary, the aim of the signal is attracting the attention of the person, and convincing to him to leave his car and follow the escape indications without delay or doubt and as quickly as possible.

In our design for emergencies, signals are located in the walls of the tunnel and have a triangular prism shape. As in Figure 4, each of the faces of the prism will indicate opposite directions, but only one of them will illuminate in the event of alarm (central control will decide this). When a row of signals are installed in a tunnel separated by tens of meters, a user will see a flashing path of attracting green signals on one side and no lights at the other side. This effect is accentuated by the prismatic shape that conceals the unlit side; this constructive volume eases the lateral visibility (more common in a tunnel) and accompanies the correct orientation. This way, the signal's design fulfills two main required functions: To attract attention indicating the right direction and reducing the response time and to confirm right direction as a person moves, clearing any doubts he/she should have and thus reducing movement time.



Figure 4. Render and signal prototype.

Our proposed implementation also considers the use of phosphorescent materials, due its obligatory use in different safety regulations [52]. Such materials allow capturing ambient light to ensure a minimum visibility in darkness, which makes the signal highly reliable, as it is a basic physical phenomenon. It should be noted that these materials present limited use when there is not enough ambient light to charge them, as in a tunnel environment. Accordingly, we propose using LED-based retro-illumination to periodically excite them, in order to keep minimum luminescence—in case of failure of the internal lighting—and to provide full intensity and maximum contrast in emergency situations [53].

As in Figure 5, internally the signal has three layers: first there is a plate with the opaque mask with the pictogram's negative; behind there is a sheet of phosphorescent translucent methacrylate; and then an LED panel backlight.

With this design, we control the energy transferred to the phosphorescent material, which will then be released in an uncontrolled but predictable manner. Thus, we go beyond regulatory guidelines, providing additional features such as remotely controllable dynamic messages, use in low lightning scenarios, energy

efficiency that allow battery operation simplifying infrastructure, installation, and ensuring operation in emergency situations with no-electricity situations.



Figure 5. Signal layers scheme: pictogram, retro-reflective, photo-luminescent, and LED layers.

3.1.2. Electronics

The Smart Signal itself is composed of two elements: a “traditional” signal (Figure 5) and an electronic device, which manages the signal. This electronic device has sensory, load control (used to handle the retro-illumination panels), communication and intelligent capabilities. This way, electronic and “traditional” signal become complementary, being possible to add Smart Thing capabilities to a signal previously installed or, even, to market them separately.

In order to explain the electronic device design, it has been divided into several functional blocks (Figure 6). The next sections explain these blocks in more detail.

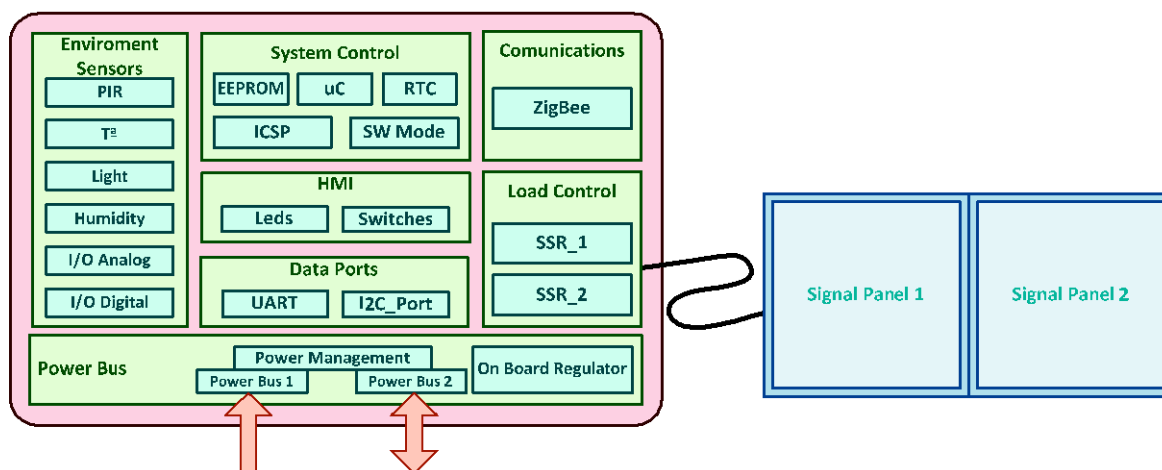


Figure 6. Block diagram of the electronic device.

Power Management

This device has two power inputs, which enables to implementing different configurations.

1. Single power supply without backup battery: Power supply is provided through power bus 1 and power bus 2 is unplugged.

2. Single power supply with backup battery: Power supply is provided through power bus 1 and power bus 2 is connected to a backup battery, which is continuously charging. If the power supply is unplugged, the device is powered through the backup battery.
3. Double power supply: Power supply provided through bus 1 is used to power the electronic device and bus 2 is used to power the signal display.

Currently, the Smart Signal uses the last configuration, with a Lithium-ion battery (4.2 V 4.2 Ah) connected to power bus 1 and a battery pack of 12 V 14 Ah Alkaline Batteries (with a very low self-discharge current) connected to power bus 2 (this source is used only when a warning is detected).

Load Control

Load control block is used to turn on/off the retro-illumination panel (load). These panels are based in 12 V LED technology, with a peak power consumption of 8 W by panel. In this case, a SSR (Solid State Relay) has been selected as control element, in order to provide isolation between control and load, and also because it can switch on/off quickly, supporting different working modes (short or long blink, continuous lighting, *etc.*).

Sensors

Three sensors have been included in the PCB (Printed Circuit Board) design, all of them digital, simplifying the hardware design (as filtering and conditioning blocks are not required).

- Presence sensor: The PANASONIC EW—EKMC1601111, a PIR (Passive InfraRed Sensor), has been selected as presence sensor. This sensor activates an interruption when it detects movement inside their control zone.
- Light sensor: The APDS-9301-020 from AVAGO has been selected as light sensor. This sensor is managed by an I2C interface and can measure visible and IR irradiance in two separate channels.
- Temperature and humidity sensor: The SHT21 from SENSIRION integrates a temperature and humidity sensor in one device with a good performance and low cost. It is also controlled by an I2C interface. In situations where only the temperature measurement is required, it can be replaced by the cheaper LM75.

Control

The control block is performed by a microcontroller, an EEPROM memory and a rotatory switch:

- A low cost, low power, 8 bits microcontroller, the PIC18F26J11-I/SO from MICROCHIP has been chosen as control. Also, an external 31.876 KHz Xtal has been included in order to use the microcontroller's internal RTCC (Real Time Calendar/Clock).
- To save the configuration parameters and other relevant data, a non volatile EEPROM of 8 Kbits is connected with the microcontroller by I2C.
- The rotary switch enables selecting one of the 10 preconfigured working modes.

Mesh Communications

Zigbee Communications have been implemented using the transceiver ETRX3 from Telegesis. This smart device follows a dual hardware architecture, where a low power microcontroller runs the application and controls a network co-processor implementing ZigBee Pro stack. After deep analysis and experimentation, we found this architecture more efficient in terms of power consumption than using a system on chip solution (embedding a radio module plus a programmable microcontroller), as it allows splitting tasks between two specialized microcontrollers; one for sensing tasks and the other for communication.

To integrate all these capabilities, a specific hardware has been designed (Figure 7). The design of this device is aimed to allow for both its easy use in new *Smart Signals* and the adaptation of existing traditional signal. For this, several input/output (screw terminals for easy use), and items such as jumpers (for energy management settings) and switches (for the definition of operation modes) have been included. This electronic device has been successfully used to:

- Evaluate and show the different capabilities of a *Smart Signal* (as mentioned in Section 2.2. Context Awareness).
- Develop a solution to the problem of emergency management, as it will be seen later.

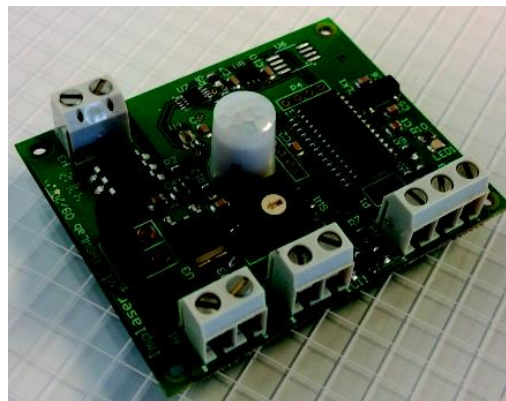


Figure 7. Electronic device.

3.2. Gateway

The *Smart Signals* communicate among them wirelessly through a mesh ZigBee network, backed by some dedicated, mains-powered devices, which route the messages exchanged (ZigBee Routers). Although in the proposed scenario, the detection of the emergency situations could be accomplished by other smart devices that would raise an alarm and would broadcast it directly through the ZigBee network, triggering of alarms has been delegated to the current tunnel security infrastructure (Figure 8).

When any of the Tunnel Security Infrastructure Elements (like smoke detectors, fire detectors, cameras, etc.) identifies a dangerous situation, it transmits that information to the Tunnel Security Infrastructure Control. There, the system itself or the operator in charge may decide to raise an alarm, which is delivered to the *Smart Signal* System through the Gateway (as well as to any other tunnel security infrastructure elements). The Gateway will broadcast the alarm message to the network, so the *Smart Signals* are notified about the emergency and react consequently. The Gateway is also in charge of typical system maintenance

tasks, such as creating the ZigBee network, *Smart Signal* discovery and recruitment, general system health monitoring, *etc.*

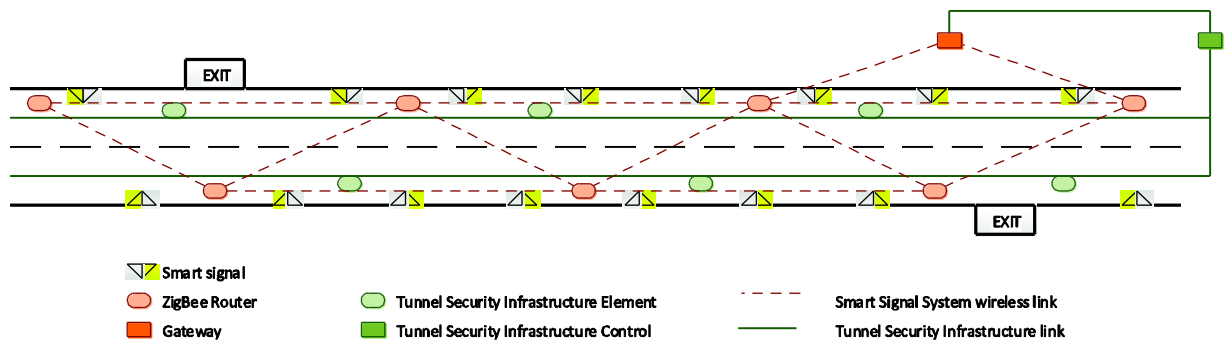


Figure 8. Smart Signal System infrastructure.

It is possible to find different proposals centered on the concept of Gateway [54]. In our case, we have used an embedded PC running Linux and a Java virtual machine where we have deployed an OSGi framework to implement the Gateway intelligence. Using OSGi as development framework eases development of the Gateway intelligence, as we can build modular software following the layered architecture depicted in Figure 9, and we may focus on one single layer when developing, while the whole application layers will be arranged at execution time. Each layer may comprise one or more bundles (isolated fragments of code that implement some behavior and are accessible to other bundles by publishing services in the OSGi framework).

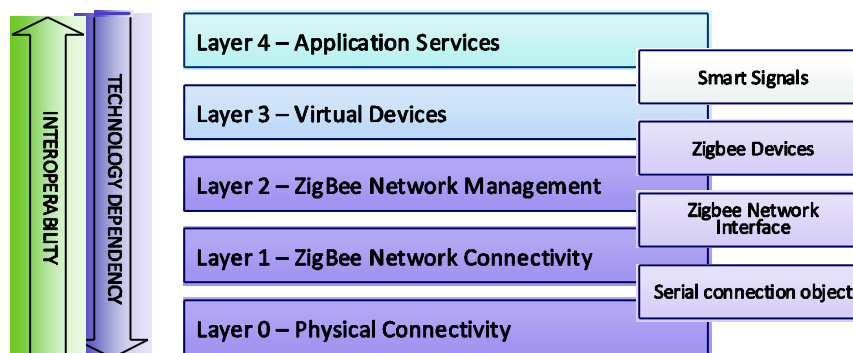


Figure 9. Gateway software architecture.

The lower layer of the architecture is in charge of providing base connectivity with the ZigBee network through a USB dongle acting as network coordinator and network sink, which results in a sort of serial connection object allowing sending and receiving bytes as data streams.

The second layer adds meaning to those bytes, implementing the specific communication protocol with the USB dongle and allowing effective communication with the ZigBee Network. This results in an object representing the ZigBee Network Interface (ZNI), which encapsulates the communication protocol with methods and fields.

The middle layer is in charge of managing the ZigBee network through the usage of the ZNI representation service, being able to discover ZigBee devices on the network, recruit them and handle

network unavailability. At this layer, objects representing ZigBee devices are available, although they are already described in terms of the underlying technology.

In the next layer, objects related to ZigBee devices are described as Virtual Devices, regardless of their underlying technology, and whether they represent Smart Signals.

The upper layer is devoted to Application Services, which use those Virtual Devices to provide the main Gateway intelligence. Specifically, there is a component (bundle) that offers a GUI allowing the operation of the Smart Signal System in a local fashion, and another component that creates a MODBUS slave and translates Smart Signals objects into a process image shared with the Tunnel Security Infrastructure Control, which behaves as the MODBUS master.

This architecture also allows easily adding other services, such as local processing of the information gathered by the Smart Signals (for example, with the temperature information provided by them, it would be possible to better characterizing the compromised area in fire-related alarms), or exposing that information not only through MODBUS, but other interfaces, without affecting existing functionalities.

4. Performance Evaluation

We performed evaluation of the system at various levels:

4.1. Lab Testing

Phosphorescent material can be considered a transitory repository of energy, similar to how batteries accumulate electrical energy. *Smart Signal* should wisely use its energy to provide required service with the minimum energy expenditure. Evidently, LED lighting will spend most of the energy, thus there is a number of important parameters to be decided in order to be the most efficient. We set up an experimentation bench to analyze signal performance measuring energy consumption and luminance variation in time. Figure 10 shows the panel used when it has no light source or luminescence, when illuminated using rear LEDs and when fully charged of phosphorescence.



Figure 10. Uses of a *Smart Signal* with phosphorescent support.

Table 1 shows the parameters studied, the design of the experiment and the results of each experiment.

Table 1. Parameters affecting the efficiency of Smart Signal with phosphorescent support.

Parameters	Experiment Design	Results																																																									
Wavelength and relaxation time	Excitation with white, blue and ultraviolet LEDs																																																										
		<table border="1"> <thead> <tr> <th>Light source</th> <th>Initial Radiation intensity (mcd)</th> <th>Excitation time (s)</th> <th>Electrical Energy Spent (joules)</th> <th>Initial rad. Intensity performance (mcd/joule)</th> <th>Radiated Intensity (cd·s)</th> <th>Radiated Intensity performance (cd·s/joule)</th> </tr> </thead> <tbody> <tr> <td>White LED</td> <td>19,700</td> <td>160</td> <td>2090</td> <td>9.43</td> <td>1276.36</td> <td>0.61</td> </tr> <tr> <td>Violet LED</td> <td>19,700</td> <td>120</td> <td>842.4</td> <td>23.33</td> <td>1176.28</td> <td>1.40</td> </tr> <tr> <td>Blue LED</td> <td>19,700</td> <td>120</td> <td>745.2</td> <td>26.45</td> <td>1150.19</td> <td>1.54</td> </tr> <tr> <td>UV LED</td> <td>19,510</td> <td>180</td> <td>518.4</td> <td>37.64</td> <td>1093.54</td> <td>2.11</td> </tr> </tbody> </table>	Light source	Initial Radiation intensity (mcd)	Excitation time (s)	Electrical Energy Spent (joules)	Initial rad. Intensity performance (mcd/joule)	Radiated Intensity (cd·s)	Radiated Intensity performance (cd·s/joule)	White LED	19,700	160	2090	9.43	1276.36	0.61	Violet LED	19,700	120	842.4	23.33	1176.28	1.40	Blue LED	19,700	120	745.2	26.45	1150.19	1.54	UV LED	19,510	180	518.4	37.64	1093.54	2.11	<p>We can observe that UV light requires the minimum energy to get same initial radiation intensity; around 25% of white and 70% of blue light. It can be also observed that although the initial radiation is roughly the same (19,700 mcd), the radiated energy provided during one hour is slightly larger for the white light This provokes that ratios of energetic performance of radiated energy in one hour to become better for white light, but still very far from UV.</p>																					
Light source	Initial Radiation intensity (mcd)	Excitation time (s)	Electrical Energy Spent (joules)	Initial rad. Intensity performance (mcd/joule)	Radiated Intensity (cd·s)	Radiated Intensity performance (cd·s/joule)																																																					
White LED	19,700	160	2090	9.43	1276.36	0.61																																																					
Violet LED	19,700	120	842.4	23.33	1176.28	1.40																																																					
Blue LED	19,700	120	745.2	26.45	1150.19	1.54																																																					
UV LED	19,510	180	518.4	37.64	1093.54	2.11																																																					
Intensity and excitation time	Excitation of UV LED with different energy (variation of power and time) from 43 J to 518 J	<table border="1"> <thead> <tr> <th>Voltage (V)</th> <th>Excitation time (min)</th> <th>Current (A)</th> <th>Electrical Energy Spent (joules)</th> <th>Initial Radiation intensity (mcd)</th> <th>Initial rad. intensity performance (mcd/joule)</th> <th>Radiated Intensity (cd·s)</th> <th>Radiated Intensity performance (cd·s/joule)</th> </tr> </thead> <tbody> <tr> <td>12</td> <td>1</td> <td>0.24</td> <td>172.80</td> <td>9720.0</td> <td>56.25</td> <td>612.53</td> <td>3.54</td> </tr> <tr> <td>12</td> <td>2</td> <td>0.24</td> <td>345.60</td> <td>16,900.0</td> <td>48.90</td> <td>973.04</td> <td>2.82</td> </tr> <tr> <td>12</td> <td>3</td> <td>0.24</td> <td>518.40</td> <td>19,510.0</td> <td>37.64</td> <td>1093.54</td> <td>2.11</td> </tr> <tr> <td>11</td> <td>4</td> <td>0.13</td> <td>343.20</td> <td>12,500.0</td> <td>36.42</td> <td>852.68</td> <td>2.48</td> </tr> <tr> <td>10</td> <td>4</td> <td>0.08</td> <td>192.00</td> <td>5182.0</td> <td>26.99</td> <td>522.45</td> <td>2.72</td> </tr> <tr> <td>9</td> <td>4</td> <td>0.02</td> <td>43.20</td> <td>778.0</td> <td>18.01</td> <td>100.58</td> <td>2.33</td> </tr> </tbody> </table>	Voltage (V)	Excitation time (min)	Current (A)	Electrical Energy Spent (joules)	Initial Radiation intensity (mcd)	Initial rad. intensity performance (mcd/joule)	Radiated Intensity (cd·s)	Radiated Intensity performance (cd·s/joule)	12	1	0.24	172.80	9720.0	56.25	612.53	3.54	12	2	0.24	345.60	16,900.0	48.90	973.04	2.82	12	3	0.24	518.40	19,510.0	37.64	1093.54	2.11	11	4	0.13	343.20	12,500.0	36.42	852.68	2.48	10	4	0.08	192.00	5182.0	26.99	522.45	2.72	9	4	0.02	43.20	778.0	18.01	100.58	2.33	<p>It shows how lowering the radiated light power reduces the performance in terms of initial radiation. It happens similarly with radiated intensity but not so evident when saturating the luminescent material. Both evidences indicate that powering LEDs at nominal level is recommended and also exciting material little time.</p>
		Voltage (V)	Excitation time (min)	Current (A)	Electrical Energy Spent (joules)	Initial Radiation intensity (mcd)	Initial rad. intensity performance (mcd/joule)	Radiated Intensity (cd·s)	Radiated Intensity performance (cd·s/joule)																																																		
12	1	0.24	172.80	9720.0	56.25	612.53	3.54																																																				
12	2	0.24	345.60	16,900.0	48.90	973.04	2.82																																																				
12	3	0.24	518.40	19,510.0	37.64	1093.54	2.11																																																				
11	4	0.13	343.20	12,500.0	36.42	852.68	2.48																																																				
10	4	0.08	192.00	5182.0	26.99	522.45	2.72																																																				
9	4	0.02	43.20	778.0	18.01	100.58	2.33																																																				
Excitation frequency	Maintaining LED energy, modify excitation frequency from continuous to 100 Hz	<table border="1"> <thead> <tr> <th>Frequency (Hz)</th> <th>Excit. Time (min)</th> <th>Electrical Energy Spent (joules)</th> <th>Initial Radiation intensity (mcd)</th> <th>Initial rad. intensity performance (mcd/joule)</th> <th>Radiated Intensity (cd·s)</th> <th>Radiated Intensity performance (cd·s/joule)</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>2</td> <td>345.60</td> <td>16,900.0</td> <td>48.90</td> <td>973.04</td> <td>2.82</td> </tr> <tr> <td>5</td> <td>4</td> <td>345.60</td> <td>9020.0</td> <td>26.10</td> <td>669.72</td> <td>1.94</td> </tr> <tr> <td>50</td> <td>4</td> <td>345.60</td> <td>6073.0</td> <td>17.57</td> <td>549.83</td> <td>1.59</td> </tr> <tr> <td>100</td> <td>4</td> <td>345.60</td> <td>5961.0</td> <td>17.25</td> <td>550.97</td> <td>1.59</td> </tr> </tbody> </table>	Frequency (Hz)	Excit. Time (min)	Electrical Energy Spent (joules)	Initial Radiation intensity (mcd)	Initial rad. intensity performance (mcd/joule)	Radiated Intensity (cd·s)	Radiated Intensity performance (cd·s/joule)	0	2	345.60	16,900.0	48.90	973.04	2.82	5	4	345.60	9020.0	26.10	669.72	1.94	50	4	345.60	6073.0	17.57	549.83	1.59	100	4	345.60	5961.0	17.25	550.97	1.59	<p>Spending the same energy but modulating it in different ways has a considerable impact in performance being continuous excitation the most efficient.</p>																					
		Frequency (Hz)	Excit. Time (min)	Electrical Energy Spent (joules)	Initial Radiation intensity (mcd)	Initial rad. intensity performance (mcd/joule)	Radiated Intensity (cd·s)	Radiated Intensity performance (cd·s/joule)																																																			
0	2	345.60	16,900.0	48.90	973.04	2.82																																																					
5	4	345.60	9020.0	26.10	669.72	1.94																																																					
50	4	345.60	6073.0	17.57	549.83	1.59																																																					
100	4	345.60	5961.0	17.25	550.97	1.59																																																					

Considering that we have a primary battery reservoir of 12 V and 14 Ah and that we need 2 min of continuous excitation of UV LED consuming 345 joules (or white LED consuming 1567 joules) to get 10 min of acceptable luminescence, we can have 292 h of signaling (64 h with white LED). Thus, laboratory test confirmed the feasibility of a battery-operated signal that can guarantee a considerable level of visibility (much higher than traditional emergency signals) in an environment with little ambient light as a tunnel.

4.2. Field Testing

For the evaluation of the system, several tests in the tunnel Monrepos I (roadway N330 of Autonomous Community of Aragon, Spain) have been conducted. The tunnel is a monotube tunnel with three traffic lanes, a length of 1449 m (a fifth of Aragon by length), and built in the 1990s for improving access to the Aragonese Pyrenees. After being qualified as one of the least safe tunnels in Spain [55], it has undergone a security check and upgrade. In July 2014 (a few weeks before its reopening), a fully functional prototype of the proposed emergency signaling system was deployed. Previously, characterization tests for ZigBee wireless communications, which are not the subject of this article, has been done in the same tunnel.

The tunnel control center was emulated with a laptop controlling the rest of the system. This point was located in the first emergency exit tunnel (KP1.400); from there, the rest of the system was deployed (Figure 11) in an incremental way. This area was selected because it coincides with a curving stretch (one of the sections most complicated due to blocking the propagation of radio frequency). The rest of test setup consisted of:

- Eight routers: Separated approximately 250 m from each other, alternately placed in the wall on either side (preliminary tests showed that this was the best configuration).
- Twenty prototypes of *Smart Signal*: Separated approximately 50 m each other alternately placed in the wall on either side. So from 3 to 7 *Smart Signal* depended on each router.

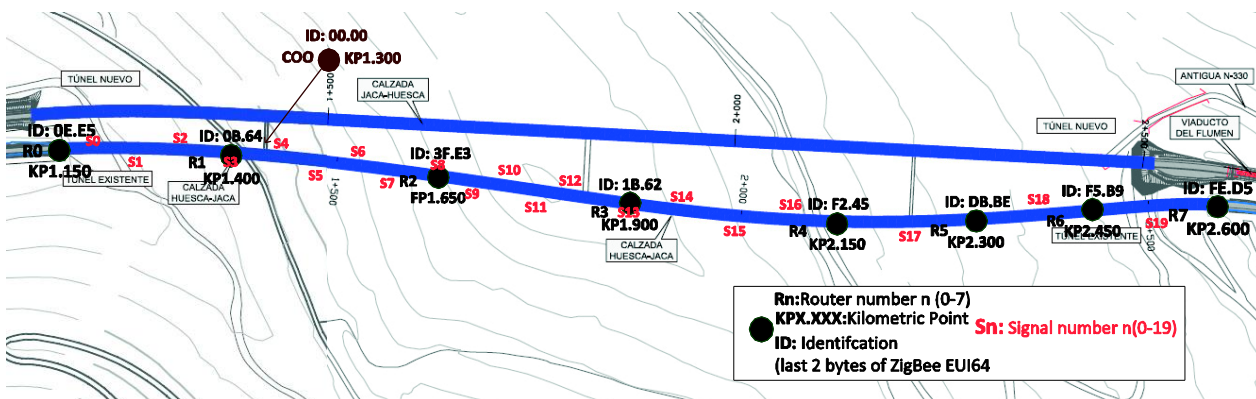


Figure 11. Distribution of routers and *Smart Signals* in Monrepos I tunnel.

Below (Figure 12) is a detail of the part of the deployment around coordinator station, corresponding with the section aimed at assessing the “signal element” and its interaction with the user:

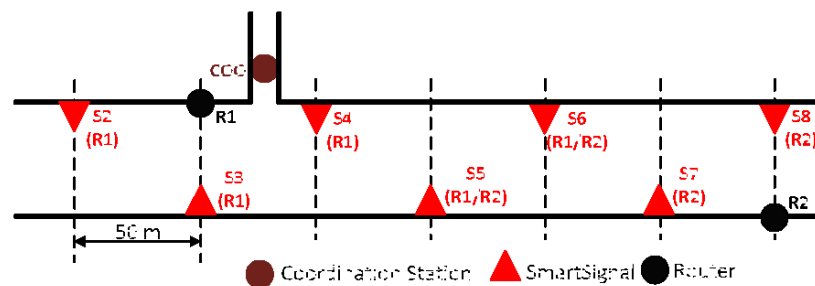


Figure 12. Details of setup around coordination station (scenario to test the perception).

When placing different elements of the system along the tunnel, the next distance must be considered:

- Distances between routers, $D_{Routers}$, will be such that for each deployment and RF settings (transmission power and antenna), in case a router falls, the infrastructure remains intact. This assumes that the minimum radius of coverage of each router is at least $2 \times D_{Router}$.
- Distance between signals is defined by the applicable regulations. In the deployment shown, managers of the tunnel set the separation between signals at 50 m.
- Distance between signal and a router: The electronic design ensures that the minimum coverage of each signal is $D_{Routers}$, so in case a routers, the signal associated with it can immediately connect to the next.

For ensures correct distances, the RF characteristics of the devices are:

- Router: External $\frac{1}{2}$ 50 Ω antenna (BKR2400 Embedded Antenna Design Ltd.), output power of 10 dBm and sensitivity of -106 dBm.
- Signal: On Board 50 Ω antenna (Ceramic Rufa Antenova), output power of 7 dBm and sensitivity of -100 dBm.

It should be noted that the maximum power of emission for European Compliance is 10 dBm (10 mW), and for FCC, IC Compliance is 20 dBm. The ZigBee transceiver used allows up to 22 dBm for routers and 8 dBm for signals.

The deployment process was carried out in the following steps:

1. Installation of coordinator station (emulator of the tunnel control center).
2. Installation of routers.
3. Establish communications infrastructure.
4. Placing prototype of *Smart Signal* near wall, alternately placed in the wall on either side.
5. Connecting and checking of signals connectivity. Fixing signals in wall.

A similar process will be follow to deploy a definitive installation of the system. Figure 13 shows a picture of the real deployment of the system.



Figure 13. Snapshot during setup process. The closest signal (hanging on the wall) is turned off and the rest are turned on.

The proposed system is not aimed to detecting an emergency, but to improve the monitoring of the tunnel in a normal situation, and to provide additional information during an emergency situation.

- Temperature, humidity and light sensors report useful environmental information to the control staff of the tunnel in normal situations. In emergency situations, these parameters can provide additional information about the evolution of fire along the tunnel.
- Presence sensors allow for extracting information about the traffic along the tunnel in normal situations. Its main use is to detect activity in time bands outside the scheduled time of high traffic density. During an emergency situation, it is assumed that in certain environments this sensor will not be useful (as in fires, since sources of intense heat, or movement of thermal mass impede its operation), however it is very useful in proximity to emergency exits to estimate the level of influx of people.

In addition, the versatility of both the architecture and the *Smart Signal* allows for:

- On the one hand, to incorporate external sensors to the *Smart Signal* through the inputs provided for this purpose. During the deployment of the system, limit switch, proximity switch (for detecting emergency doors opened), and the external smoke sensors have been evaluated.
- Furthermore, to incorporate other devices into the system and take advantage of the communications infrastructure, we are currently working on the inclusion of a mobile sensor (and exploring its positioning capability).

Once the system was operating, various evaluation tests were conducted, focusing on the following aspects.

4.2.1. User Perception Testing

The objective of these tests was to determine the validity of the final service offered by the system, abstracting from the technology. In a specific area of the tunnel, which we will call demonstration area, we carried out the following tests:

- Surveys to qualified staff (manager of the tunnel, maintenance operators, manager of a signalization company and expert in security from the Spanish Ministry) about their feelings of the system.
- Self-evaluation by the developers themselves.

- Simulation of user's interaction with the signaling system. To this end, a group of users, underwent to the assessment of different predefined scenarios, in each of them:
 1. The evaluator placed one user at a point in the tunnel.
 2. The evaluator established secretly the location of a hypothetical emergency exit.
 3. The user is informed by the evaluator that there is an alleged fire and must find the emergency exit.
 4. The evaluator activates the signaling system and prompts the user to try to get to the hypothetical emergency door following the indications of emergency signaling system.
 5. During the progress of evaluation, the evaluator accompanied the user, logging their behavior and timing. At certain points in the tunnel (previously defined), the evaluator asks several questions (noninvasively with the test) about signal perception.

Thus, each of these trials consists of a path of the user accompanied by the evaluator, along the demonstration area. Seven situations were raised (with different parameters and circumstances). Figure 14 shows an example of three scenarios (1, 2, 3) evaluated. In each of them, there is the user's start position (green circle X.1), and other positions where the user's behavior must be analyzed and the evaluator registers the elapsed time. If the user enters the shaded area, a negative test result is considered.

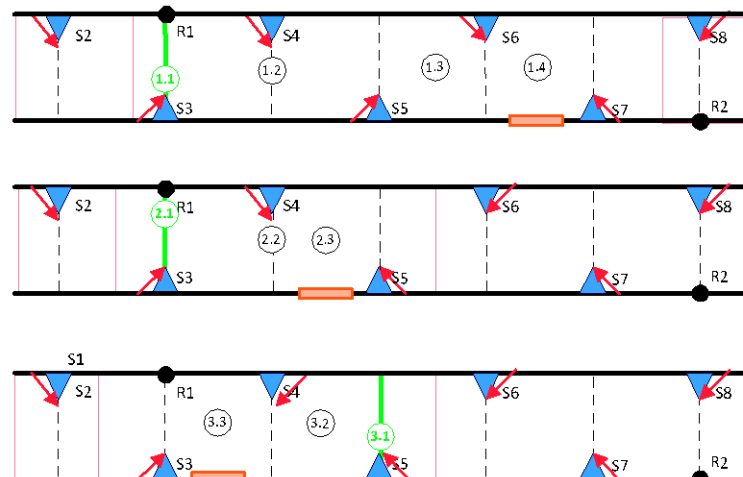


Figure 14. Examples of scenarios for simulating an emergency (in each of them, the emergency exit is a virtual point only known to the evaluator).

In summary, we can say that all the tests about user perception resulted favorably, hence the system is considered a remarkable advance over existing signaling systems.

4.2.2. Technical Testing

The objective of these tests is to characterize aspects of the technology used, which are impossible to evaluate in the laboratory (mainly regarding wireless communications in a tunnel). Various tests were conducted, and we have implemented a series of test benchmarks that run automatically in the coordinator station to analyze different aspect of the system. We discuss below the most important ones.

Routing and Behavior of the System When Communications Infrastructure Falls

Routes are calculated automatically and dynamically, based on the best link power. A tunnel is a particularly complex environment, so previous studies were conducted to characterize the ZigBee communications. It is worth mentioning that the nature of this environment explains some unexpected behavior *a priori*, such as the link between nodes (FE.D5) and (0B.64) shown in Figure 15. The link is through a direct connection despite being the longest route, due to the topology of the tunnel (nearby routers to FE.D5 have the worst connectivity due to the curvature of the tunnel), and an area with electromagnetic noise in nearby routers was also detected. The road condition has been periodically monitored as a measure of network quality.

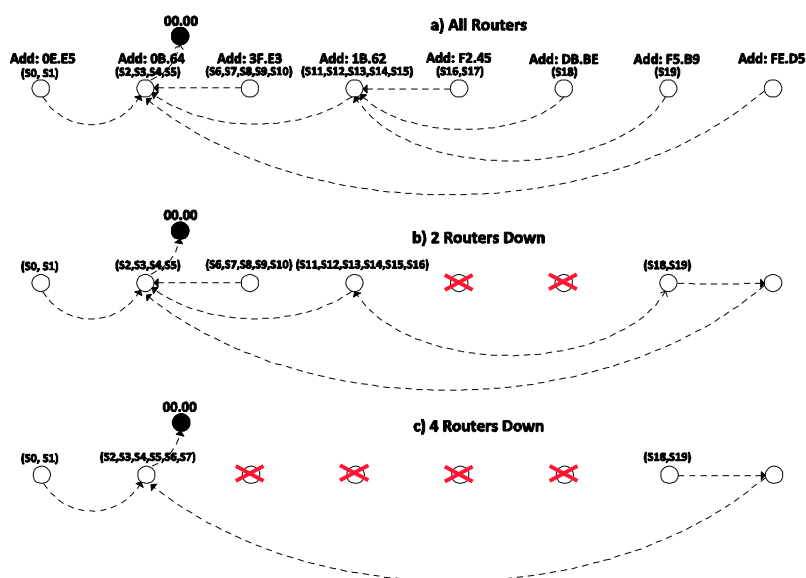


Figure 15. Routes and signals that depend on each router: (a) Initial snapshot; (b,c) simulating successive drop of nodes.

In addition, to evaluate the behavior in a failure scenario, the disconnection of several routers have been done simulating that they are destroyed. One advantage of the proposed system is its resilience, since in case of fire, although some of the routers fail (because they may be located in an area affected by the emergency), the system calculates the new routes, so unaffected areas remain operational. Additionally, as a measure of redundancy, the possibility of using several nodes prepared to adopt the role of coordinator could be contemplated, so that if the network is segmented, the system can still operate into independent networks.

Data Latency

Message latency quantifies the availability of a *Smart Signal* in order to exchange information with it. We consider this availability from a total perspective (including all the layers), and define it, as how much time is required to force a *Smart Signal* to acknowledge a ping from the upmost layer of the *Smart Signal* Infrastructure. With this, latency depends on the following factors: processing time at the Gateway, number of hops between the gateway and the *Smart Signal*, time elapsed by the *Smart Signal* in Sleep mode, and

the processing time in the Smart Thing. Both processing times are negligible compared with the other two parameters. Figure 16 shows the results, where we can see a direct relation between the latency and the number of hops.

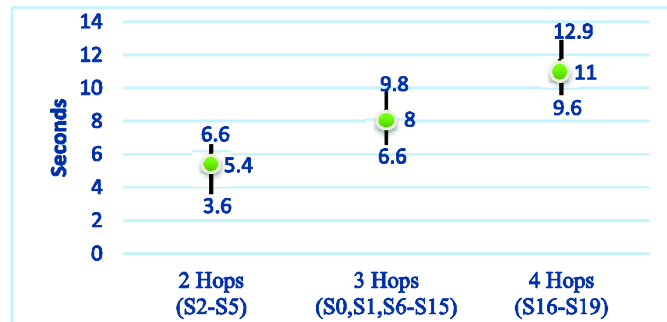


Figure 16. Latency intervals (within a 95% interval) of signals.

Data efficiency

It is common to consider the quality of a communication network as the relation between lost messages and total messages. For a global evaluation of the system, it is preferable to consider both ends of the system instead of point-to-point connections, thus we use the messages generated by the *Smart Signal* while sensing the environment *versus* the amount of data received in the gateway for a defined operation time. To calculate this value, we use only deterministic events (a scheduled predefined routine of monitoring in the Smart Signal) so the total data to be generated are well known *a priori*. In our case, the accumulated data efficiency is 95.3% (Table 2). It has been found that, in general, errors are due to unexpected problem with communications.

Table 2. Data efficiency.

Number of Smart Signals	20
Smart Signal reporting rate	1 data/min
Operation time	4 h
Expected total messages	4800
Actual messages received	4574 (95.29%)
Messages lost	227 (4.73%)

5. Conclusions

Signals are habitual elements present in cities. Therefore, it seems natural to consider them as important building blocks of the future Smart City. Moving from today's signals (which are seen merely as passive and simple elements) to *Smart Signals* (with communication, sensing and improved user interaction capabilities), might turn the city's signals into the main information channel of the Smart City.

However, to date, there is no proposal to use signals as main actors in the Smart City, nor to consider them as something with *more possibilities*. Thus, this paper presents the concept of the *Smart Signal* as the natural evolution of signaling in the context of the future Smart City, and as first class citizens on the Internet of Things ecosystem.

A conceptual model of *Smart Signal* inspired in the well-known model of *Smart Thing* has been proposed, highlighting the specific additional requirements related to signaling in terms of the interaction with the user. Based on this model, we have reviewed the technical features that a *Smart Signal* should have, mainly focusing on energy issues and wireless communications.

To validate the *Smart Signal* concept, an implementation in the context of a tunnel emergency signaling system has been presented, describing in detail the design and implementation of the *Smart Signal*, and its integration into a Smart Signaling System, as well as its deployment in a real setup, the Monrepos I tunnel (Aragón, Spain) in a fully operational way.

The *Smart Signal* and the Smart Signaling System have been evaluated exhaustively, both technically and functionally, evidencing its feasibility and its advantages over classical signaling. Actually, there is a perception that the system is very close to real use with a high chance that it will be turned into a commercial product.

The advantages of such *Smart Signal* concept are multiple. First, the actual functionality of the signal is significantly improved, and moreover new capabilities for interaction with users of the signals will be offered. Furthermore, there are some critical situations where there is no optimal solution currently, and in which a *Smart Signal* as the proposed could be an efficient and optimal solution. Second, *Smart Signals* could turn into the natural sensory mechanism of the Smart City, as communication and energy issues are the main constraints of Smart City objects, and aggregating sensing and signaling on the same component may significantly decrease the costs of Smart City infrastructure. Third, incorporation of *Smart Signals* to the Smart City may open the door to new services that will increase quality of life and safety of smart citizens.

Acknowledgments

The authors would like to acknowledge Implaser for their support and Memory Lane project funded by Spanish Ministry of Science and Technology.

Author Contributions

All authors were involved in the foundation items. All authors wrote the paper and read an approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References and Notes

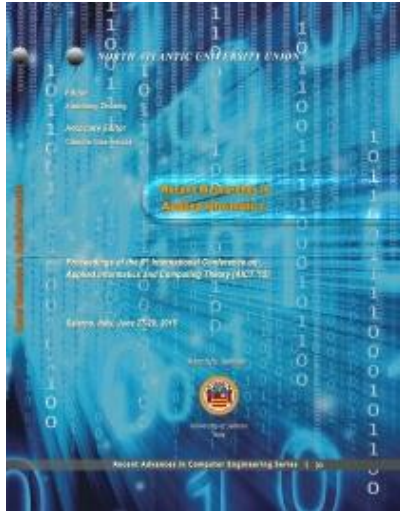
1. Suárez, N. Señalización de emergencia en túneles carreteros y ferroviarios. *Obras Urbanas October 2009*, 76–79.
2. Ronchi, E.; Nilsson, D. *Interim Report: Traffic Information Signs, Colour Scheme of Emergency Exit Portals and Acoustic Systems for Road Tunnel Emergency Evacuations*; Department of Fire Safety Engineering: Lund University, Lund, Sweden, 2013.

3. Leccese, F. Remote-Control System of High Efficiency and Intelligent Street Lighting Using a ZigBee Network of Devices and Sensors. *IEEE Trans. Power Deliv.* **2013**, *28*, 21–28.
4. Elejoste, P.; Angulo, I.; Perallos, A.; Chertudi, A.; Zuazola, I.J.G.; Moreno, A.; Azpilicueta, L.; Astrain, J.J.; Falcone, F.; Villadangos, J. An Easy to Deploy Street Light Control System Based on Wireless Communication and LED Technology. *Sensors* **2013**, *13*, 6492–6523.
5. Minnesota, U. University of Minnesota-Smart Signal. [En línea]. Available online: <http://signal.umn.edu/> (accessed on 30 April 2015).
6. National Institute for Advanced Transportation Technology. (National Institute for Advanced Transportation Technology). Smart Signals: Enabling Traffic Controller Technology. November 2006.
7. VAISALA. VAISALA-Road Solutions. [En línea]. Available online: <http://www.vaisala.com/en/roads/Pages/default.aspx> (accessed on 30 April 2015).
8. Martín, F.J.L. Panel Luminoso de Señalización Vial. Spain Patente U200901552, 10 November 2009.
9. García, M. Disposición de Emisores Ópticos Y Acústicos Aplicable Para la Información de Accesos y Salidas de Túneles, Pasos a Nivel Y Similares. Spain Patente U200200099, 1 June 2002.
10. Sistema de Iluminación Para Señales de Tráfico. Patente P9601957, 22 January 1999
11. Erke, A.; Sagberg, F.; Hagman, R. Effects of route guidance variable message signs (VMS) on driver behaviour. *Transp. Res. Part F: Traffic Psychol. Behav.* **2007**, *10*, 447–457.
12. Streitz, N. Smart Future Initiative. [En línea]. Available online: <http://www.smart-future.net/3.html> (accessed on 30 April 2015).
13. IBM. Wellcome to the Smarter City. IBM. [En línea]. Available online: http://www-03.ibm.com/innovation/us/thesmartercity/index.shtml?cm_mmc=agus_brsmartcity-20090929-usbrb111_-_s_-_genhpmerch_-_sp (accessed on 30 April 2015).
14. International Electrotechnical Commission. Orchestrating Infrastructure for Sustainable SmartCities. Published in Geneva, Switzerland. 2014. Available online: <http://www.iec.ch/whitepaper/pdf/iecWPsmartcities-LR-en.pdf> (accessed on 12 June 2015).
15. ISO/IEC. Smart Cities: Preliminary Report. 2014. Available online: http://www.iso.org/iso/smart_cities_reportjtc1.pdf (accessed on 12 June 2015).
16. Al-Ali, A.R.; Zualkernan, I.; Aloul, F. A Mobile GPRS-Sensors Array for Air Pollution Monitoring. *IEEE Sens. J.* **2010**, *10*, 1666–1671.
17. Nasirudin, M.A.; Za'bah, U.N.; Sidek, O. Fresh water real-time monitoring system based on Wireless Sensor Network and GSM. In Proceedings of the IEEE Conference on Open Systems (ICOS2011), Langkawi, Malaysia, 25–28 September 2011; pp. 354–357.
18. Leccese, F.; Cagnetti, M.; Calogero, A.; Trinca, D.; di Pasquale, S.; Giarnetti, S.; Cozzella, L. A New Acquisition and Imaging System for Environmental Measurements: An Experience on the Italian Cultural Heritage. *Sensors* **2014**, *14*, 9290–9312.
19. Leccese, F.; Cagnetti, M.; Trinca, D. A Smart City Application: A Fully Controlled Street Lighting Isle Based on Raspberry-Pi Card, a ZigBee Sensor Network and WiMAX. *Sensors* **2014**, *14*, 24408–24424.
20. Tan, Y.K.; Huynh, T.P.; Wang, Z. Smart Personal Sensor Network Control for Energy Saving in DC Grid Powered LED Lighting System. *IEEE Trans. Smart Grid* **2013**, *4*, 669–676.

21. Information Society Technologies Advisory Group (ISTAG). Orientations for EU ICT R&D & Innovation beyond 2013. 2011. Available online http://cordis.europa.eu/fp7/ict/istag/documents/istag_key_recommendations_beyond_2013_full.pdf. (accessed on 12 June 2015).
22. Gimeno, A.; Marco, A.M.; Marín, R.B.; Nebra, R.C. Protocol and Architecture to Bring Things into Internet of Things. *Int. J. Distrib. Sens. Netw.* **2014**, *2014*, 158252:1! 158252:18.
23. Nakashima, H.; Aghajan, H.; Augusto, J.C. *Handbook of Ambient Intelligence and Smart Environments*; Springer: New York, NY, USA, 2010.
24. Böhlen, M.; Frei, H. Ambient Intelligence in the City Overview and New Perspectives. *Handb. Ambient Intell. Smart Environ.* **2010**, 911!938, doi :10.1007/978-0-387-93808-0_34.
25. Makonin, S.; Bartram, L.; Popowich, F. A Smarter Smart Home: Case Studies of Ambient Intelligence. *Pervasive Comput.* **2013**, *12*, 58!66.
26. Cagnetti, M.; Leccese, F.; Trinca, D. A New Remote and Automated Control System for the Vineyard Hail Protection Based on ZigBee Sensors, Raspberry-Pi Electronic Card and WiMAX. *J. Agric. Sci. Technol. B* **2013**, *3*, 853!864.
27. Bhuvaneswari, N.; Sujatha, S.; Yamuna, R. Vibrant Ambient Intelligent System for Traffic Congestion Control in Coimbatore City. In Proceedings of the 12th International Conference on Networking, VLSI and Signal Processing (ICNVS'10), Stevens Point, WI, USA, 12 October 2010.
28. Cristophe, B. Semantic profiles to model the "Web of Things. In Proceedings of the Seventh International Conference on Semantics, Knowledge and Grids, Beijing, China, 24! 26 October 2011.
29. Barontib, P.; Pillaia, P.; Chook, V.W.; Chessab, S.; Gotta, A.; Hua, Y.F. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Comput. Commun.* **2007**, *30*, 1655!1695.
30. Reite, G. Wireless connectivity for he Internet of Things: One size does not fill all. Available online: <http://www.ti.com.cn/cn/lit/wp/swry010/swry010.pdf> (accessed on 12 June 2015).
31. Watteyne, T.; Pister, K.S.J. Smart cities through standards-based wireless sensor networks. *IBM J. Res. Dev.* **2011**, *55*, 80!89.
32. Chang, K.-H.; Mason, B. The IEEE 802.15.4g Standard for Smart Metering Utility Networks. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5! 8 November 2012.
33. Asensio, Á.; Blasco, R.; Marco, Á.; Casas, R. Hardware Architecture Design for WSN Runtime Extension. *Int. J. Distrib. Sens. Netw.* **2013**, *2013*, 136745:1! 136745:11.
34. Rabaey, J.; Ammer, J.; Otis, B.; Burghardt, F.; Chee, Y.H.; Pletcher, N.; Sheets, M.; Qin, H. Ultra-Low-Power Design: The roadmap to desappearing electronics and ambient intelligence. *IEEE Circuits Devices Mag.* **2006**, *22*, 23!29.
35. Piguat, C. *Low-Power Electronics Desig*; CRC Press: London, UK, November 2004.
36. Arabi, K. *Low power Design Techniques in Mobile Processors*; CRC Press: London, UK, 2004.
37. Shearer, F. *Power Management in Mobile Devices*; CRC Press: London, UK, 2008, p. 336.
38. Ka mierski, T.J.; Beeby, S. *Energy Harvesting Systems: Principles, Modeling and Applications*; Springer: New York, NY, USA, 2011; p. 176.
39. Sudevalayam, S.; Kulkarn, P. Energy Harvesting Sensor Nodes: Survey and Implications. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 443!461.

40. Leccese, F.; Cagnetti, M. An Intelligent and High Efficiency Street Lighting System Based on Raspberry-Pi Card, ZigBee Sensor Network and Photovoltaic Energy. *Int. J. Eng. Sci. Innov. Technol. (IJESIT)* **2014**, *3*, 274!285.
41. Penella-López, M.T.; Gasulla-Forner, M. *Powering Autonomous Sensors. An Integral Approach with Focus on Solar and RF Energy Harvesting*; Springer: New York, NY, USA, 2011.
42. Tan, Y.K.; Panda, S.K. Energy Harvesting From Hybrid Indoor Ambient Light and Thermal Energy Sources for Enhanced Performance of Wireless Sensor Nodes. *IEEE Trans. Ind. Electron.* **2011**, *58*, 4424!4435.
43. Afsar, Y.; Sarik, J.; Gorlatova, M.; Zussman, G. Evaluating Photovoltaic Performance Indoors. In Proceedings of the 38th IEEE Photovoltaic Specialists Conference (PVSC), Austin, TX, USA, 3! 8 June 2012.
44. Tan, Y.K.; Panda, S.K. Self-Autonomous WSN with wind energy harvesting for remote sensing of wind-driven wildfire spread. *IEEE Trans. Instrum. Meas.* **2011**, *60*, 1367!1377.
45. Sardini, E.; Serpelloni, M. Self-powered wireless sensor for air temperature and velocity measurements with energy harvesting capability. *IEEE Trans. Ind. Electron.* **2011**, *60*, 1838! 1844.
46. Zuo, L.; Tang, X. Large-Scale vibration energy harvesting. *J. Intell. Mater. Syst. Struct.* **2013**, *24*, 1405!1430.
47. Vázquez-Rodríguez, M.; Jiménez, F.; de Frutos, J. Modeling Piezoelectric Harvesting Materials in Road Traffic Applications. In *Mathematical Models and Methods in Modern Science*; World Scientific and Engineering Academy and Society (WSEAS): Tenerife, Spain, 2011.
48. Vettri y G. Kausthubh. Green Energy-EZOWATT. In Proceedings of the 2011 2nd International Conference on Environmental Science and Technology IPCBEE, Singapore, 2011.
49. OSGI Alliance. OSGI Alliance Web site. [En línea]. Available online: <http://www.osgi.org/Main/HomePage> (accessed on 30 April 2015).
50. Fridolf, K.; Nilsson, D.; Frantzich, H. Fire evacuation in underground transportation systems: A review of accidents and empirical research. *Fire Technol.* **2013**, *49*, 451!475.
51. Martens, M. Human Factors Aspects in Tunnels: Tunnel User Behaviour and Tunnel Operators. EU FP5 Contract G1RD-CT-2002-766, 2008.
52. AENOR, EN ISO 7010:2012. 2010.
53. Laborda, C.H.; Laborda, V.H.; Pardo, J.I.A.; Lozano, J.P.; Bascuas, T.B.; Gimeno, Á.A.; Marín, R.B.; Nebra, R.J.C.; Marco, Á.M. Señal con retroiluminación inteligente y autónoma. España Patente U201230980, 21 September 2012.
54. Qiu, P.; Zhao, Y.; Heo, U.; Zhang, D.; Choi, J. Gateway Architecture for Zigbee Sensor Network for Remote Control over IP Network. In Proceedings of the 8th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT), Kuching, Malaysia, 15! 18 June 2010.
55. Aragon, D.d.A. Fomento adjudica por 97,2 millones el tramo Alto de Monrepós-Caldearenas». [En línea]. Available online: <http://www.diariodelaltoaragon.es> (accessed on 30 April 2015).

2.5 WIRELESS SENSOR NETWORKS IN TRAFFIC MANAGEMENT SYSTEMS



Ángel Asensio, Carlos A. Trasviña-Moreno, Rubén Blasco, Álvaro Marco, Roberto Casas

Proceedings of the 6th International Conference on Applied Informatics and Computing Theory (AICT'15)

2015

RESUMEN:

En este trabajo se presenta la propuesta sobre la que se está desarrollando el proyecto MoVVI que pretende desarrollar un sistema inteligente que realice una gestión más eficiente del tráfico y la ocupación de los espacios viarios.

El marco de aplicación supone nuevos retos, como una mayor área de cobertura o la necesidad de interactuar con sistemas ya existentes. Para dar respuesta a estas nuevas necesidades se propone el concepto de u-Cloud. Si una NoT “Manuscrito 3 (Interoperabilidad)” agrupaba a elementos que compartían la misma tecnología de comunicaciones, con el concepto de u-Cloud se pretende encapsular a dispositivos de múltiples tecnologías de comunicación (agrupando de cierto modo varias NoT). Un concepto adicional es que el Gateway de una u-Cloud dispondrá de comunicaciones con un rango de cobertura mayor (cientos a miles de metros) de modo que estos podrán comunicarse ente si. Con ello el Gateway de una u-Cloud puede conectarse tanto a Internet como directamente a otra u-Cloud. En cierto modo, puede verse como una propuesta para crear varias células dentro de un despliegue de IoT. Adicionalmente, en el marco de este trabajo se empiezan a investigar los protocolos LPWA.

Wireless Sensor Networks in traffic management systems

Á. ASENSIO, C. TRASVIÑA-MORENO, R. BLASCO, Á. MARCO, R. CASAS*

Department of Electronics and Communication Engineering,
University of Zaragoza

Campus Rio Ebro, María de Luna, 3 50018
SPAIN

* rcasas@unizar.es <http://howlab.unizar.es/>

Abstract: - Citizen wastes an important part of their life moving around a city, considering that most of these displacements are in vehicles, it could be said that good traffic conditions suppose a better quality of life and less environmental contamination. Thus, traffic management systems are one of the most important systems of a city. Nowadays, TICs are being incorporated so as to evolve to the Smart City. One of these technologies are the wireless sensor networks, which grants us awareness of our surrounding context. For traffic management systems, the true state of the context is reviewed, as it is critical for optimal management. Regarding this, it is logical to incorporate wireless sensor network into traffic management systems. This paper has presented the progress made so far in the MOVVI project, which aims to develop a smart traffic management system for an optimum control of the occupation of spaces in cities.

Key-Words: *Smart City, Wireless Sensor Network, Traffic management*

1 Introduction

The continued increase in greenhouse gas levels in the atmosphere, due to human activity, has raised the temperature level of the planet drastically in recent years. Current forecasts project an upsurge in global temperature between 0.1°C and 0.2°C by decade, causing significant global climate changes [1]. This situation, as well as the increasing price of fossil fuels, has greatly stimulated research in green energy sources. Although in the long term the substitution of fossil fuels for other energy sources is the best solution, in short term, those alternatives which contribute to reasonable and sustainable energy management may also impact greatly.

Analysing the greenhouse gas emissions (Fig. 1), the contribution made by the transportation sector can be appreciated, as it one of the most important.

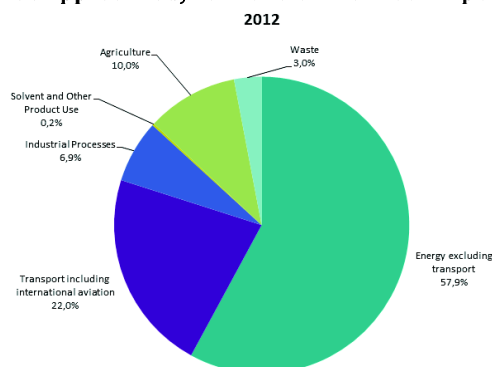


Fig. 1 Greenhouse effect gas emissions by sector [2].

The constant increase in vehicle numbers in Europe (e.g. in Spain, according to Eurostat, in 1991 the motorization rate, cars per 1000 inhabitants, was 321, compared to 476 in 2012) [2] and, in general the rest of industrialized countries, has diminished the air quality of our cities, being one of the main causes of pollution in the aforementioned.

The current state of events has led many municipalities to take restrictive measures against contaminating vehicles: London and Stockholm have introduced tolls, Berlin or Lisbon do not allow vehicle circulation in downtown areas, whilst in France similar measures are being considered for their main cities [3].

Since the birth of the semaphore in 1868 in London, the use of regulation technology has augmented progressively. Nowadays devices like information panels, light signals, radars, video cameras, etc. are of common nature both in cities and intercity routes. Nonetheless, most of the current traffic supervision systems follow a time-based pattern for semaphore management, which adjusts according to the hour, day and season of the year. The emergence of Smart Environment technologies in these scenarios, such as Wireless Sensor Networks (WSN), Distributed Artificial Intelligence (DAI), cloud computing, smartphone apps, etc. offer a wide array of opportunities for technology innovation in these fields.

In this context, the MoVVI project [4] proposes an innovative solution. Based on the concept of Internet of Things (IoT), in which every device is interconnected, the creation of a smart and ubiquitous WSN is proposed. The aforementioned will be able to report data to control traffic centers or private space managements (e.g. parking lots, tollgates, etc.), as well as public data bases that will allow data mining from third party applications (e.g. smartphone apps, web services, etc.).

2 Traffic scenario

Different technologies are involved in the design of a traffic system management. In this brief state of the art we focused on sensors, traffic regulation elements and information panels. These devices are found present in the traffic scenario reporting current context information to the system, controlling and regulating traffic lights, and providing information to users, either pedestrian or vehicle drivers. Also, since our approach comes from a Smart Environments point of view, WSN applications, context modelling, interoperability and software architecture are been considered.

2.1 Conventional sensors

Induction-loop traffic sensor is one of the most used methods in traffic monitoring applications. Its operation is based on the change in inductance that occurs when a vehicle (or a metallic object) passes through or stops on the electromagnetic field generated [5]. When a change is detected, the vehicle count is increased. This technology has two main problems: its relatively high installation cost (system needs to be wired and requires a traffic stoppage for some time) and it has a high rate of breakage which increase maintenance costs.

Another technology that is increasing day by day its relevance in the traffic management are the vision systems due to the increment of current computational capabilities. Algorithms for vision systems enable license plate recognition, pedestrian detection, vehicle speed estimation, etc., further providing the traffic management body a direct point of view of the road [6]. Usually, these systems are used as speed sensors, and to monitor large traffic areas (e.g. crosses, tunnels, etc.), controlling limited access areas where the traffic is restricted, such as parking access. Cameras, however, present some disadvantages such as: acceptance issues by users, prone to vandalism, fixed infrastructure access requirements (IP or electrical grid), maintenance and, their main drawback, high cost.

Other systems use pressure changes produced by vehicles treading the asphalt to monitor traffic. They range from traditional pressure hose vehicle counter sensor that is attached to the asphalt surface and used to perform specific studies bounded in time, to other permanent systems, such as optical fiber based embedded on asphalt [7]. This latter system base their operation on the reduction of conductivity caused by the crushing of the fiber. Both these systems present similar problems as those of inductive coils.

In the last years, magnetic sensor appeared as an alternative to the traditional induction-loop sensors. These tiny devices, which are usually wireless, are placed inside the asphalt [8]. Its operation is based on the detection of perturbations of the magnetic field that occurs when a metal object passes over them. This technology, beyond vehicle enumeration, is used also to monitor parking places [9]. These devices typically have a higher durability than induction-loops, however, they require more maintenance (battery replacement about every 5 years) and are more expensive.

Although these are the most used technologies, it is possible to find other traffic sensors for specific applications, as infrared barriers to monitor a single lane or, more innovative systems, as the implemented in the city of Zaragoza (Spain), which detects Bluetooth devices present in the cars and calculates the time of arrival to the different points of the city [10].

2.2 Traffic control and signalling elements

In this case, the emergence of technologies based on LEDs has represented one of the most important advances in this field. Their low power consumption has made possible the installation of information panels without main power access, using solar panels at those points where the rising cost of it justified its replacement. This same situation has occurred at traffic lights which mostly have been replaced by LED-based devices due to the significant energy savings. In the case of information panels, the mass use of LEDs has meaningfully reduced its cost, being increasingly used in both urban and interurban roads.

Currently, the *Dirección General de Tráfico* (DGT), main authority in traffic management in Spain, classify their user information system in the next categories: Before the trip (teletext, internet, etc.), during the trip (information panels, RDS-TMC), in any moment (by phone, Radio traffic, auto-guided).

2.3 Context modelling, interoperability and software architecture

Usually, wireless sensor networks communicate with fixed infrastructures through a *Gateway*. This device behaves as the connection point between physical elements (sensors, actuators, etc.) and their equivalent virtual elements (models of the devices in order to be handled by the control software).

In the *Things* world, interoperability among devices from different manufacturers is constrained to the use of standard communication protocols which intend to connect them seamless, such as 6lowPAN, RFID, WIFI, or 3G. Other protocols like ZigBee or Bluetooth deepen on the interoperability issue, establishing how the data interchange for some applications should be, by defining application profiles. For example, this allows for a phone supporting the Bluetooth Headset Profile (HSP) the use of any manufacturer's Bluetooth headset directly. Regarding sensors and actuators, although the IEEE1451 standard [11] proposes a schema to use them independently from their communication technology, nowadays its introduction into the market is minimal.

Focussing on the virtual representation of devices and following the *Internet of Things* (IoT) paradigm [12], where every object has a counterpart on the Internet, there are standards and ontologies that helps modelling the context, providing virtual representations for the devices that builds *Ambient Intelligence* (AmI) environments (sensors, actuators, interfaces, etc.). Most of the standards are based on the IP protocol, but this does not ensure the required interoperability for the IoT applications. For example, standards such as the Extended Environments Marks-up Language (EEML), SensorWeb or SenseWeb use XML-based schemas in order to integrate sensors and actuators into the virtual world. However, these schemas focus only on the data modelling, lacking the semantics and ontologies required to turn them into valid tools for making a complex information processing and adapting to a higher abstraction level. Initiatives such as COSE [13] or Dogont [14], among others, propose different ontologies and approaches to model objects (sensor, actuators, interfaces, appliances, etc.) on smart environments, formalizing the devices and binding their contents by semantic relations, and offering access to them through web services.

It should be noted also that most of this initiatives are based on the *Open Services Gateway initiative*

(OSGi) [15]. The increasing use of OSGi in new applications and consumer goods, as well as the use of Service Oriented Architectures (SOA), is strongly related with the need of durable and easy to update technologies. Development of monolithic software applications in these context is expensive and not sustainable in the mid-term, and it is here where SOA allows for the development of, easy to update, modular applications.

In that sense, OSGi proposes a framework where the code is arranged into bundles that can be managed dynamically. These bundles can be devoted to specific tasks, and communicate each other by means of services published within the framework. This architecture allows to maintain and evolve each of these bundles separately, integrating their full life-cycle (code, build, install, activate, deactivate, update...) without requiring even to stop the entire application [16], [17].

2.4 WSN application

Sensor networks are one of the most common tools used in DAI deployments, as they offer a wide array of possibilities for environmental monitoring in non-invasive self-powered devices. They are comprised of several elements (sensors, actuators, communication modules, etc.) which aim to communicate information to a higher system for data mining and decision making.

The use of communication protocols such as ZigBee, Bluetooth or custom tailored solutions are common amongst WSN, as they allow for enhanced device energy autonomy. WiFi, although less frequent, is also utilized in these type of systems due to its widespread popularity in urban environments and its newly added low energy consumptions features. The previously mentioned protocols also offer different network topologies (tree, star, mesh, etc.), which allow implementations ranging from a few simple nodes to highly complex systems.

Applications for WSN are very heterogeneous, covering a wide spectrum of work areas. Implementations have been made for remote patient health monitoring [18], irrigation and fertilization of crop fields [19], electrical grid power management for household buildings [20], natural disaster prevention [21], amongst others.

Traffic control is not oblivious to these systems, as presented by Sharma et al. [22]. The aforesaid can be found applied in smart traffic control systems for traffic jam detection, optimum route search or assisted parking, amongst others. Various studies [23], [24] lay out guidelines for systems which

dynamically adjust the semaphore interaction based on data provided by a given WSN. Others [9], [25], [26] focus on parking space availability, utilizing various sensors to detect vehicle movement to offer real-time space management. Yet few have been able to address both issues in a single smart and intuitive WSN system.

3 The MoVVI approach

3.1 System description

Main objective of the MoVVI Project is to develop a *Smart City Application* able to manage traffic and parking places more efficiently than current systems. The system is based on a Wireless Sensor and Actuator Network (WSAN) embedded in the environment, which will enable the municipalities, citizens and traffic control centres to access enhanced information, thus optimizing the use of vehicles (decreasing traffic jams, optimizing routes, times and information). Additionally, it may suggest alternatives to the use of particular vehicles according to current traffic conditions.

Initially, a scenario is proposed where sensors, and optionally, control and signalling elements will be deployed on points of interest on streets, parking and roads. Those devices will be grouped into small area networks, called *u-Clouds* in the context of the project, which will use low power wireless technologies such as ZigBee, and will include dedicated Gateways that will provide Internet connectivity and access to the related municipality management network.

This architecture is highly scalable and considers just covering a small area or the monitorization of an entire city and their metropolitan area. The smart sensors will feed the municipal database as well as Internet open databases with information in several degrees of detail. Thanks to the use of these, it will be possible to account the number of vehicles passing through a specific section, to discriminate the type of vehicle, to detect vehicles driving against the traffic, to estimate the average speed on the road, to monitor the occupancy on parking places, etc.

In the case of big cities, this system deepens into the concept of Smart Cities, allowing municipalities for a better management of parking or access restricted areas, and even offering advanced services such as planning or public reservation of these areas. On the other side, the availability of public databases with the traffic information, will allow the

development of information applications by the citizens who wish to do so.

The platform will be designed with the objective of allowing for easily adding new sensors compatible with standard communication protocols, as well as increasing the Internet-connected sensor *u-Clouds* communication infrastructure, and enabling covering other additional needs. Collected data will be processed on the Cloud, and will produce high level information that will be used by municipality managers to enhance space management, as well as it could be offered to third parties for developing their own applications. All this data will be integrated natively into the urban control application for big cities developed within the project, or integrated into any other application by means of an external API.

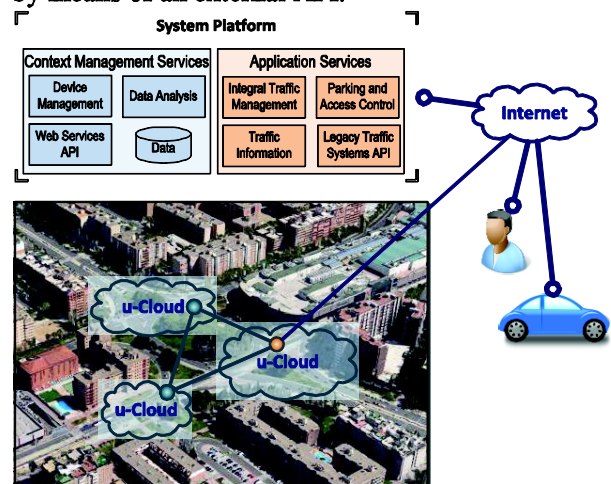


Fig. 2. System architecture

The general architecture of the system is depicted in Fig. 2. A number of *u-Clouds* are deployed on the scenario, and collect data from the sensors that are shared among them through their Gateways. Any of the *u-Cloud* Gateways with Internet connectivity behaves as connection point between the physical world and the remote platform, where Context Management Services and Application Services reside. Context Management Services are in charge of tasks related with information retrieval, analysis and storage, as well as device management, and provides an API for accessing that context data. Application Services are in charge of the specific tasks related to the traffic and parking management, as well as the communication with the legacy traffic management systems already installed. Users may also interact with the services provided by the platform through the Internet.

The overall operation of the system can be better understood with the example proposed in Fig. 3.

Here, the system consisting of a Gateway, several routers and a number of traffic sensors which creates a mesh network is presented. Information displays and semaphores are also considered, although the latter are not accessed directly from within any u-Cloud, but the remote platform. Traffic sensors aligned in the same lane allow to: monitor lane occupancy; estimate maximum, average and minimum speed; detect wrong-way traffic; count the amount of vehicles; or identify vehicle typology (providing the number of shafts). This information allows for tuning dynamically semaphore regulation in order to alleviate traffic.

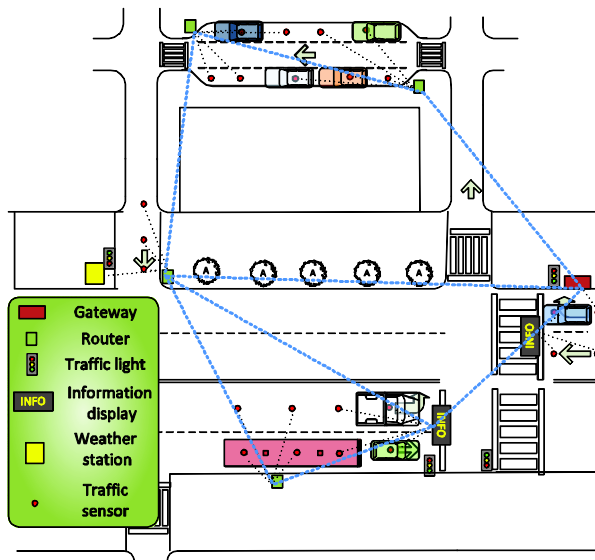


Fig. 3. Use case: urban environment.

The same kind of traffic sensor is deployed on the parking places to detect their usage, and the information about available parking places on secondary streets is reported to the users through the information displays present on the main street.

3.2 u-Cloud

A u-Cloud is composed, generally, by a router which is the central element of a u-Cloud, several sensors, information displays and actuators.

This router is ready to support several RF protocols, amongst others such as Bluetooth and ZigBee which simplifies the communication with a broad spectrum of sensors. In order to enable the interoperability at the application level, as we explain in section 3.2.2 all devices use the Common Thing Protocol, (CTP). Each u-Cloud could be able to take its own decision depending on the context. This is possible due to the router "intelligence" and data-storage capabilities, being able to implement simple algorithms and pre-processing the sensors information. This situation

approaches the system to the paradigm of the Fog Computing.

New Wireless Magnetic sensors are been developed in the MoVVI project. These sensors have two main functionalities: traffic and car parking monitoring. Beyond these traffic sensors, u-Cloud enables the connectivity of any kind of CTP sensor.

u-Cloud is able to support wireless CTP information displays and actuators, though integration is done at platform level, since this infrastructure should be previously installed in the city.

In the next section the main u-Cloud issues related with wireless communications, interoperability and an application example are presented.

3.2.1 Wireless communications

WSN technology represents a significant commercial interest in the current context, being one of the key players in the development of Smart City [27]. This situation is producing a coexistence of wireless protocols that usually ends with the interconnection of the WSN to a fixed infrastructure (Internet) based on IP (Internet Protocol)[28]. In this environment, technologies based on IEEE802.15.4, 6LoWPAN and IPv6 are combining to meet this demand [29], [30].

Depending on the application, it is critical to select the most appropriated technology for wireless connectivity comparing them in terms of coverage, data throughput, network topology or energy consumption. In any case, the more data you need to exchange, the further you need to communicate, the more time you need to be online, the more energy you need, and consequently the quicker you will run out of batteries

Sensors are usually powered by batteries, and their installation is complicated, so it is of great interest that their autonomy be as high as possible. Therefore, the main guideline when selecting its wireless technology is low consumption. The ZigBee protocol (into 2.4GHz band) has been selected as an alternative due to its ability to work with different types of network topology, enough bandwidth (250kbts/s), bearable latency times, adequate coverage range (+500m with LRS option) and, also, it is a standard widely established on the market.

Focusing on the MoVVI project it is possible to identify three levels of communication:

- Inside the u-Cloud. The u-Cloud is an Ultra-Low Power Wireless Sensor Network (ULPWSN) which includes all the

communication between the traffic sensors and the closest router. In this area, there has been an intensive development of custom devices that use RF protocols of short range, in the past few years. This enables a market with great availability of a wide range of devices for covering different needs.

- Between u-Clouds. This level of communication could be consider as a Wireless Neighbourhood Area Network (WNAN) and includes the communication between routers and Gateway in a mesh network based on ZigBee
- Between the Gateway and the IP world (Wide Area Network, WAN)

¡Error! No se encuentra el origen de la referencia. presents our technological proposal and shows its communication levels.

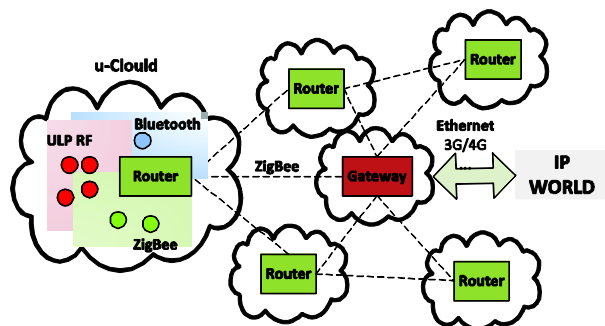


Fig. 4. u-Cloud communications levels

The system architecture is built around the router of each u-Clouds. These routers, are part of the ZigBee network that interconnects the u-Clouds to each other and with the Gateway. Additionally, the routers of the u-Cloud that may require it, will support other protocols. Explicitly, the protocols that have been considered as additional are Bluetooth and the low frequency RF protocols of existing devices. The adopted solution allows the inclusion of new communication protocols, both internally into u-Cloud, and between u-Clouds. In regard to the latter case, the joint use (even the replacement) of ZigBee with other technologies such as WiMax or LoRa, is being contemplated.

3.2.2 Interoperability

Communication standards ensure stack layer's interoperability (network management and maintenance, security, data exchange, etc.) between devices connected using the same protocol. In a u-Cloud, devices that share a common protocol could be connected directly amongst them. Moreover, the router connects devices using a wireless communication protocol with devices that have

another protocol, behaving as a translator between protocols. However, once that connectivity between devices has been achieved, to ensure interoperability, it is necessary both the exchange of data, as well as the understanding of the information embedded in the data. Aforementioned, there are several protocols that try to incorporate this "understanding of knowledge" and "abstraction of the device" to ensure the device operation and its interoperability between them.

On the one hand, not all protocols support abstractions of the device operation, and those that do, may not be efficient when operating on devices with limited resources. On the other hand, it is necessary that these abstractions are the same, so that different devices can interact with each other. We have proposed the Common Things Protocol (CTP) [31] as a solution to the problem of interoperability between heterogeneous devices in the MOVVI project.

CTP aims to provide a specification that allows interoperability among communication standards while keeping simplicity, functionality and efficiency. CTP takes into account both the existing specifications in the standards and the needs from the final applications. It integrates the strategies, concepts and terms of some of the alternatives mainly the TED (Transducer Electronic Data Sheet) concept from IEEE1451 to provide device's information and the ZigBee concepts of clusters and bindings. The definition process is approached from an ontological perspective considering that devices must perform some function while being in contact with users and context. CTP usually fulfilling the following paradigms:

- Context Interaction: embed sensors, actuators (to modify the environment) and/or simple human interfaces.
- Distributed Computing: to implement from the simplest logic to complicated services or data processing algorithms.
- Communication.

Regardless of its functionality, each thing will always "live" in a certain location and time and will have its "capabilities" (processor, communication transceiver, memory, etc.) and "restrictions" (power source, operation ranges, etc.) that are represented into the endpoint BASE of CTP. This endpoint constitutes the basic set of attributes and functionalities of any device. Depending on the specific functionalities that integrate the device, it will also implement multiple application endpoints that should be of any of the three categories of devices (derived from their capacity to interact with

the context): SENSOR, ACTUATOR or HMI. Thus, an endpoint can be defined as each of the sub-devices that have a complete functionality and, altogether with the others, build the device. Additionally, a cluster is defined as a set of commands, events and responses which together define a communication interface between two endpoints. Commands are usually action requests to an endpoint (of the same or different kind) that should send back a response informing about the action result; e.g. ask for a sensor value and get it back. The ontology defines attributes which are implemented in the protocol as GET/SET requests and responses. Events are asynchronously generated messages sent to previously subscribed endpoints. CTP describes a reduced and simple communication interface defining the meaning type and range of the parameters when needed, so CTP is self-contained and auto-defined.

CTP is encapsulated in the upper layers of existing protocols (into payloads), trying to maximize the capabilities of the native protocol. For example, if CTP is used over ZigBee, the definition of a CTP binding is done according to native capabilities of the ZigBee standard protocol. In this way, CTP can adapt to different requirements with high efficiency. Currently, CTP has been incorporated into various types of devices for development systems with different purposes, such as energy monitoring for buildings, ambient intelligences (AMIs) applied to home automation, environmental monitoring, smart signal, human interface devices, etc.

3.2.2 Example of application

Currently, we are working on the setup of a test and exhibition system in the public parking space of the campus Rio Ebro, at the University of Zaragoza (Spain). Firstly, this setup will be used to test and validate the technological developments of the project during 2 years. Finally, at the end of the project, the setup will be used to optimize the parking usage. On the one hand, it will grant detailed information of the traffic access (frequencies, traffic jams, etc.). On the other hand, it will inform users about the availability of parking places through Smartphones, internet or through the information displays, enabling new services for the University, such as controlling the load/unload parking areas, offering on line parking reservations, etc.

Focusing in the system design, as it is shown in the Fig 5, it is formed by five u-Clouds:

- u-Clouds 1 to 3 are focused in car park monitoring and each one has 24 Magnetic Zigbee traffic sensors (MZTS) placed in the parking places.

- u-Cloud 4 is formed by 8 MZTS placed in parking places, another 8 monitoring the access and an information display. This display shows the number of free parking places available in the controlled area. Also a weather station with temperature and humidity ZigBee sensor has been added to this u-Cloud.
- u-Cloud 5 is formed by three MZTS which monitoring the access area to the parking.



Fig. 5. Example of application.

Inside the u-Cloud, each router manages the connected device, checking periodically the health of each sensor. This information is sent to a platform through the Gateway (note that in this case the router placed in the u-Cloud 4 is playing the role of Gateway thanks to its access to the IP connectivity).

When a parking space changes its status, an event is sent to the remote platform which actualizes its status. This event is also used by the u-Cloud 4, which manages the information display, in order to update the number of available spaces.

Access sensors will be monitoring the number of vehicles in each line, reporting in configured intervals. Note that the sensors could work in real time, but with a high cost for their batteries.

Finally, the meteorological station, which is monitoring temperature and humidity, may use the wireless infrastructure, thanks to its CTP sensor devices, reporting periodically data to the platform.

4 Conclusion

In this paper the effect of traffic in cities, particularly its environmental impact, has been highlighted.

The scenarios in which the traffic management systems operate, have been exposed. Moreover, of current the introduction of sensors, context

modelling and WSN as mechanisms to improve the solutions present, have been reviewed.

With foregoing considerations, an approach has been carried out for the MoVVI project, presenting a novel architecture for a smart traffic management system. The architecture is designed around two basic elements, u-Clouds and Gateway, and has been focused on using wireless communications, as well as devices embedded in the environment, to interact with it

The concept of u-Clouds has been further developed as a means to handle the heterogeneity of devices, while also allowing the deployment of the infrastructure along wide spaces in the city. Two of the most critical aspects of the u-Cloud have been reviewed in great depth: wireless communications and interoperability between devices. This last aspect presents its self as a challenge, thus the use of a self-developed protocol (CTP), which has been tested successfully on previous projects, has been proposed as a solution., and

Finally is showed the example that currently is getting ready to fine-tune the technology and analyze results.

Acknowledgements: Spanish Ministry of Economy and Competitiveness, project MoVVI (RTC-2014-2425-4) and Memory Lane (TIN2013-45312-R)

References:

- [1]I.P.O.C. Change, "Climate change 2007: The physical science basis," *Agenda*, vol. 6, pp. 07 2007.
- [2]Eurostat. *Statistical office of the European Union* [Online]. available: <http://ec.europa.eu/eurostat>.
- [3]M. García. Contaminantes ¡¡Fuera!! *Tráfico y seguridad vial. Dirección General de Tráfico. Ministerio del Interior. Gobierno de España.* pp. 36-38.
- [4]iASoft, Kepar and I3a. *Movvi | Movilidad Verde Inteligente* [Online]. available: <http://movvi.iasoft.es/>.
- [5]L.A. Klein, M.K. Mills and D.R. Gibson, *Traffic Detector Handbook*, FHWA-HRT-06-139 ed., 2006.
- [6]A. Mogelmose, M.M. Trivedi and T.B. Moeslund, "Vision-based traffic sign detection and analysis for intelligent driver assistance systems: Perspectives and survey," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 13, no. 4, pp. 1484-1497 2012.
- [7]Sensor Line. *Fiber Optic Sensors* [Online]. available:<http://sensorline.de/pages/application-areas/road-traffic/fiber-optic-sensors.php>.
- [8]A. Haoui, R. Kavalier and P. Varaiya, "Wireless magnetic sensors for traffic surveillance," *Transportation Research Part C: Emerging Technologies*, vol. 16, no. 3, pp. 294-306, 6 2008.
- [9]E. Sifuentes, O. Casas and R. Pallas-Areny, "Wireless magnetic sensor node for vehicle detection with optical wake-up," *Sensors Journal, IEEE*, vol. 11, no. 8, pp. 1669-1676 2011.
- [10]Ling and Phil. (2011). Traffic monitoring system uses Bluetooth sensors over ZigBee. *EE Times Europe*.
- [11]IEEE, "IEEE standard for a smart transducer interface for sensors and actuators wireless communication protocols and transducer electronic data sheet (TEDS) formats," *IEEE Std 1451.5-2007*, pp. C1-236 2007.
- [12]L. Atzori, A. Iera and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787-2805 2010.
- [13]Z. Wemlinger and L. Holder, "The COSE ontology: bringing the semantic web to smart environments," in *Toward Useful Services for Elderly and People with Disabilities*, 2011, pp. 205-209.
- [14]D. Bonino and F. Corno, *Dogont-ontology modeling for intelligent domotic environments*, Springer, 2008.
- [15]OSGi Alliance. *OSGi Alliance website* [Online]. available: <http://www.osgi.org/Main/HomePage>.
- [16]Jiankun Wu, Linpeng Huang, Dejun Wang and Fei Shen, "R-OSGi-based architecture of distributed smart home system," *Consumer Electronics, IEEE Transactions on*, vol. 54, no. 3, pp. 1166-1172 2008.
- [17]Xie Li and Wenjun Zhang, "The design and implementation of home network system using OSGi compliant middleware," *Consumer Electronics, IEEE Transactions on*, vol. 50, no. 2, pp. 528-534 2004.
- [18]S. Jung, R. Myllyla and W. Chung, "Wireless machine-to-machine healthcare solution using android mobile devices in global networks," *IEEE Sensors Journal*, no. 13, pp. 1419-1424 2013.
- [19]A.Z. Abbasi, N. Islam and Z.A. Shaikh, "A review of wireless sensors and networks' applications in agriculture," *Computer Standards & Interfaces*, vol. 36, no. 2, pp. 263-270 2014.
- [20]N.K. Suryadevara, S.C. Mukhopadhyay, S. Kelly and S.P.S. Gill, "WSN-based smart sensors and actuator for power management in intelligent

- buildings," *IEEE Transactions on Mechatronics (Early Access Article)*, doi, vol. 10 2014.
- [21]D. Chen, Z. Liu, L. Wang, M. Dou, J. Chen and H. Li, "Natural disaster monitoring with wireless sensor networks: A case study of data-intensive applications upon low-cost scalable systems," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 651-663 2013.
- [22]A. Sharma, R. Chaki and U. Bhattacharya, "Applications of wireless sensor network in Intelligent Traffic System: A review," in *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, 2011, pp. 53-57.
- [23]C. Abishek, M. Kumar and P. Kumar, "City traffic congestion control in Indian scenario using wireless sensors network," in *Wireless Communication and Sensor Networks (WCSN), 2009 Fifth IEEE Conference on*, 2009, pp. 1-6.
- [24]C. Wenjie, C. Lifeng, C. Zhanglong and T. Shiliang, "A realtime dynamic traffic control system based on wireless sensor network," in *Parallel Processing, 2005. ICPP 2005 Workshops. International Conference Workshops on*, 2005, pp. 258-264.
- [25]J. Chinrungrueng, U. Sunantachaikul and S. Triamlumlerd, "Smart parking: An application of optical wireless sensor network," in *Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on*, 2007, pp. 66-66.
- [26]R. Kumar, N.K. Chilamkurti and B. Soh, "A comparative study of different sensors for smart car park management," in *Intelligent Pervasive Computing, 2007. IPC. The 2007 International Conference on*, 2007, pp. 499-502.
- [27]D.T. Ferrandis, S.S. Climent and V. Payaá, "Enabling quick deployment wireless sensor networks for smart cities," in *Factory Communication Systems (WFCS), 2012 9th IEEE International Workshop on*, 2012, pp. 83-86.
- [28]J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey," *Computer networks*, vol. 52, no. 12, pp. 2292-2330 2008.
- [29]K. Chang and B. Mason, "The IEEE 802.15. 4g standard for smart metering utility networks," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, 2012, pp. 476-480.
- [30]T. Watteyne and K.S. Pister, "Smarter cities through standards-based wireless sensor networks," *IBM Journal of Research and Development*, vol. 55, no. 1.2, pp. 7: 1-7: 10 2011.
- [31]Á Asensio, Á Marco, R. Blasco and R. Casas, "Protocol and architecture to bring things into internet of things," *International Journal of Distributed Sensor Networks*, vol. 2014 2014.

3 CONCLUSIONES Y TRABAJO FUTURO

3.1 CONCLUSIONES

De acuerdo con los objetivos expuestos anteriormente, se han realizado aportaciones prácticas que contribuyan al desarrollo de IoT. En la presente tesis se aporta una visión extendida y transversal de IoT, tratando de integrar todos los niveles de su arquitectura, pero con especial atención en las Cosas.

Se ha llevado a cabo una revisión del estado del arte y modelización de las Cosas. Ambas han servido de base para contextualizar el objetivo principal de la tesis: la interoperabilidad y optimización energética para las Cosas. Posteriormente, se ha abordado el diseño, desarrollo e implementación de sistemas IoT que integren las aportaciones anteriores. Durante el desarrollo de la tesis, se ha puesto de manifiesto la necesidad de disponer de mecanismos de evaluación, por lo que se han realizado propuestas de métricas para tal fin.

De modo pormenorizado, las aportaciones más importantes derivadas del trabajo contenido en esta tesis doctoral, se pueden agrupar en las siguientes áreas:

- Contextualización de IoT.
- Bajo consumo.
- Interoperabilidad
- Métricas.
- Implementación de soluciones IoT.

A continuación, se describen las contribuciones específicas en cada una de estas áreas.

3.1.1 CONTEXTUALIZACIÓN DE IOT: SITUACIÓN ACTUAL Y EXPECTATIVAS

IoT es un concepto novedoso que se encuentra en plena evolución y gira en torno a la agregación de múltiples tecnologías. Nadie duda de su capacidad para ofrecer nuevos servicios y de su potencial para cambiar la sociedad actual. Por todo ello, a la hora de trabajar en este ecosistema tecnológico es necesario realizar una contextualización del mismo. Durante el desarrollo de la tesis, y a raíz de las necesidades surgidas en diferentes proyectos de investigación, se ha ido manteniendo una revisión del estado de la técnica, del contexto social y del mercado. Al respecto cabe mencionar la importancia de conocer las capacidades de las tecnologías actualmente implicadas, las herramientas de desarrollo y especialmente las barreras con las que actualmente se encuentra IoT cuando se debe implementar un sistema real y operativo. La revisión

tecnológica sobre optimización energética e interoperabilidad de las Cosas en IoT ha sido abordada respectivamente en “Manuscrito 1 (Eficiencia HW)” y “Manuscrito 3 (Interoperabilidad)” Estos conocimientos han sido de utilidad a la hora de afrontar el desarrollo de casos prácticos de servicios IoT como los mostrados en “Manuscrito 2 (IoT Energy Awareness)”, “Manuscrito 4 (Smart Signal)” y “Manuscrito 5 (WSN Trafico)”. Una perspectiva global de la situación actual desde un punto de vista más económico y social de IoT se aporta, en Anexo 4.4 “Visión económica y social de IoT resultados”.

Como se ha indicado, el campo de aplicación de IoT es muy amplio, siendo la Smart City uno de los de mayor impacto. En “Manuscrito 4 (Smart Signal)”, se ha realizado una revisión de las interrelaciones entre Smart City e IoT. Se ha avanzado en el ámbito de la eficiencia energética en edificios a través de la interacción con sus usuarios como se muestra en “Manuscrito 2 (IoT Energy Awareness)”, la señalización inteligente presentada en “Manuscrito 4 (Smart Signal)”, y posteriormente la gestión de tráfico introducida en “Manuscrito 5 (WSN Tráfico)”. Todos estos campos de aplicación presentan sinergias, y se enmarcan en varios proyectos del grupo de investigación.

3.1.2 APORTACIONES AL BAJO CONSUMO

Se ha puesto de evidencia cómo la independencia energética de los dispositivos es clave en la consecución de la ubicuidad de los mismos (tanto espacial como temporal). Las Cosas tienen limitaciones reales, siendo la necesidad de energía una de las más restrictivas actualmente y que en ocasiones pasa desapercibida desde el enfoque de más alto nivel de IoT. Para un avance real de la IoT es necesario disponer de dispositivos altamente ubicuos, capaces de operar de modo transparente y en cualquier circunstancia. Las investigaciones y aportaciones de la presente tesis se han centrado en los siguientes aspectos:

- Se ha presentado una metodología en “Manuscrito 1 (Eficiencia HW)”, para el análisis de consumos en los dispositivos. Esta metodología pretende ser de aplicación universal y sencilla, por lo que destaca por definir el ciclo de trabajo en base a especificaciones estándares como IEEE1451 y ZigBee Pro.
- En base a la metodología anterior se han analizado diferentes arquitecturas de diseño hardware y métodos de operación del dispositivo, explorando las situaciones más comunes en el ámbito de los dispositivos en IoT. Se han comparado las arquitecturas SoC (System on Chip) y Dual (Microcontrolador y Transceiver), llegando a la conclusión de que el ciclo de trabajo y la tarea de sensado pueden ser críticos a la hora de indicar cuál de ellas es energéticamente más eficiente. Para cualquiera de las arquitecturas se incide en la necesidad

de tomar conciencia de un adecuado análisis energético previo, ya que el consumo de ciertas fases del ciclo de trabajo a priori obviadas, puede ser considerable.

- Se han explorado arquitecturas con topologías de alimentación que incluyan varias fuentes de energía y elementos de almacenamiento, para dar respuesta óptima a las diferentes figuras de consumo del dispositivo (consumo por procesado, consumo pulsado asociado a comunicaciones, consumo estático en modos de bajo consumo, etc.). Actualmente los resultados alcanzados están siendo el punto de partida de otra tesis. En “Manuscrito 4 (Smart Signal)” se realiza un análisis teórico y se expone un caso particular, que considera la inclusión de otras fuentes de energía en el ciclo de operación del dispositivo (mediante la liberación de energía previamente almacenada en un sustrato fosforescente).

3.1.3 APORTACIONES A LA INTEROPERABILIDAD

Junto a la independencia energética, la interoperabilidad también es un aspecto clave para el desarrollo de IoT desde el punto de vista de los dispositivos que la conforman, por ello ha sido otro de los puntos principales de esta tesis. La revisión del estado del arte, muestra que no hay unos estándares o protocolos únicos que seguir cuando se quiere integrar una Cosa en IoT. De modo que se ha propuesto un protocolo para facilitar la interoperabilidad entre las Cosas basado en la naturaleza de las mismas.

- En “Manuscrito 3 (Interoperabilidad)” se abordan los aspectos básicos de la interoperabilidad revisando los diferentes niveles que intervienen y analizando las alternativas actuales al respecto. Se propone el uso de una arquitectura basada en un *Gateway* que permite la conexión de todas las Cosas de una misma red con Internet. Este mismo *Gateway*, es también a la vez el mecanismo para vencer la heterogeneidad de las diversas NoT. Esta solución, es acorde con la mayoría de las propuestas actuales y adicionalmente favorece una filosofía de trabajo que evita la proliferación de redes ad hoc para cada nuevo dispositivo. Existe la tendencia de que cada proveedor de dispositivos ofrezca su propio *Gateway* para conectarlo a Internet, lo que puede llevar a la existencia de un elevado número de subredes. Por el contrario, el concepto de NoT incentiva que las Cosas se integren en redes ya existentes.

Se ha desarrollado CTP como un protocolo para asegurar la interoperabilidad entre las Cosas. Esta propuesta se ha realizado de modo integrador, considerando los protocolos actuales, y las necesidades reales. Su definición se basa en una representación ontológica de las Cosas, con un enfoque de la interacción entre las mismas, y con especial énfasis en la consideración de sus limitaciones físicas. El resultado ha sido un protocolo escalable (basado

en el concepto de *cluster*) en el que se ha perseguido el equilibrio entre el mundo de las Cosas e Internet. CTP, no sustituye a ningún protocolo, sino que pretende ser encapsulado de forma sencilla en algunos de los estándares ya existentes, de hecho su definición considera aspectos de estándares actuales (IEEE1451, ZigBee, Bluetooth). CTP contempla la autodescripción de la naturaleza del dispositivo, interoperabilidad organizada y estructurada (a través de conceptos como *EndPoints* y *Cluster*), la simplificación de control (modos y escenarios), y cierto nivel de inteligencia distribuida (*Behavioral, Bindings*). El resultado se concreta en un conjunto de librerías firmware compactas y de fácil uso durante el diseño de diversos dispositivos. Pese a los continuos avances de los últimos años en la especificación de protocolos para IoT, la propuesta realizada en el marco de esta tesis sigue siendo vigente, capaz de evolucionar (por ejemplo se continúa desarrollando nuevos conceptos como la capacidad de enrutamiento a través de varias redes) y aplicable gracias a su perspectiva centrada en las Cosas.

- En “Manuscrito 4 (Smart Signal)” se amplían y aplican los resultados anteriores, para definir el concepto de *Smart Signal*, por el que una señal tradicional al uso, a través de la estrategia de interoperabilidad mostrada, pasa a convertirse en un elemento de IoT que puede prestar nuevos servicios en el ámbito de la Smart City.
- En “Manuscrito 5 (WSN Tráfico)” se pone de manifiesto que la solución propuesta soporta la heterogeneidad de dispositivos y redes a la vez que se propone el concepto de u-Cloud como un complemento a la idea de NoT. El concepto de u-Cloud, se introduce, como mecanismo para articular el despliegue de IoT en áreas espaciales de grandes dimensiones (como es el caso de una ciudad), siendo una u-Cloud una subárea de la extensión total. La necesidad de las u-Cloud surge debido a las distintas tecnologías de comunicación inalámbricas (y con ello sus rangos de cobertura) de los dispositivos en esta área. Una u-Cloud agrupa varias NoT con un solo Gateway que incorpora una tecnología de comunicación de largo alcance. De este modo las u-Cloud a través del Gateway pueden no solo acceder a Internet sino también comunicarse entre ellas. Se podría considerar que la u-Cloud es el análogo a una celda en las comunicaciones celulares. En definitiva, se ha avanzado en las implicaciones en el ámbito de la interoperabilidad que supone este tipo de arquitecturas.

3.1.4 APORTACIONES A LOS MECANISMOS DE EVALUACIÓN DE IOT

En relación al punto anterior, a lo largo de la investigación ha quedado patente la necesidad de disponer de mecanismos que permitan una evaluación objetiva de la calidad de la solución implementada. Tradicionalmente en el ámbito de las comunicaciones, han existido diferentes

métricas para medir sus prestaciones, algo similar ocurre en el campo del consumo energético e inclusive en la eficiencia del tratamiento de la información. IoT incorpora todas estas y más tecnologías, por lo que podría evaluarse el desempeño de una solución IoT, analizando por separado cada una de las tecnologías involucradas. Sin embargo, lo que realmente interesa es disponer de una herramienta de análisis global. En el marco de la tesis, se ha avanzado al respecto en los siguientes aspectos:

- Reflexión sobre las características de las métricas en IoT. El objetivo final es prestar un servicio, y se debe conocer como de eficiente o bueno es el mismo, teniendo en cuenta que para ello se requieren unos costes (energético, económico de inversión y mantenimiento), unas posibles infraestructuras, y que las diferentes soluciones imponen unas restricciones (tiempos de latencia, radios de cobertura, capacidad de concurrencia, estabilidad, seguridad). Estas valoraciones, incluso podrían incorporar factores más abstractos (satisfacción por el servicio prestado, capacidad de integración en servicios de terceros, potencial de creación de mercado, etc.). Idealmente, esta información se debe dar desde un enfoque multidisciplinar, objetivo y de modo que sea fácilmente calculable y comparable para las distintas implementaciones.
- Se han definido unos mecanismos para facilitar la determinación de métricas a nivel dispositivo. En “Manuscrito 3 (Interoperabilidad)” se definen y presentan métricas para evaluar el desempeño de CTP frente a otras alternativas, y en “Manuscrito 4 (Smart Signal)” se presentan mecanismos para disponer de una información inicial de la calidad del servicio desplegado. Para ello, el protocolo CTP incluye el concepto de salud del nodo, como un valor que el propio dispositivo estima a partir de las medidas de su comportamiento y la comparación con su comportamiento ideal estimado a priori.

3.1.5 IMPLEMENTACIÓN PRÁCTICA E INTEGRACIÓN DE SISTEMAS DE IOT

Resolver problemas reales, ofreciendo servicios de utilidad, y realizar el despliegue de la tecnología, su puesta a punto y seguimiento en un entorno realista es una de las formas más eficientes de aplicar y evaluar los resultados de investigación que se han ido proponiendo a lo largo de la tesis. Desde un punto de vista académico, la implementación y posterior evaluación de la tecnología, suponen el mejor modo para tomar consciencia de las limitaciones, necesidades reales e identificar nuevos retos tecnológicos. Dentro del marco de esta tesis, se han realizado las siguientes acciones:

- En el marco del proyecto “Liga Energética”, se ha desarrollado una aplicación de monitorización ambiental y energética que interacciona con los usuarios para incentivar el ahorro. Este proyecto supuso el despliegue de un sistema basado en la infraestructura propuesta, que contó con más de 100 nodos sensores (tanto de diseño propio como elementos comerciales). El trabajo de esta tesis ha estado asociado al desarrollo hardware y firmware de los dispositivos diseñado ex profeso.
- En “Manuscrito 4 (Smart Signal)” se presenta el concepto de *Smart Signal* correlándolo con el de Cosa de IoT través de CTP. Con ello se ha propuesto evolucionar las señales actuales (elementos pasivos) a *Smart Signal*, dotadas de capacidad de comunicación, sensado y capacidades de interacción mejoradas. Esta idea supone una innovación, puesto que hasta la fecha los sistemas de señalización similares no incorporaban capacidades avanzadas. Este concepto ha sido desarrollado en conjunción con la empresa Implaser, y ha dado lugar a varias patentes (Huerta et al. 2012), (Huerta et al. 2015) de las que el doctorando es coautor. El objetivo es introducir los sistemas de señalización en el ámbito de IoT, para crear lo que podría ser un importante mecanismo de recolección de información para la Smart City, gracias a la natural distribución y presencia de las señales en cualquier ciudad. Para conseguir una implantación real, los criterios de consumo energético (autonomía), interoperabilidad, y coste económico son vitales. Adicionalmente, se ha explorado la capacidad de este tipo de tecnologías en entornos adversos, en este caso en un túnel carretero, para lo cual se ha realizado un despliegue real, utilizando estrategias y herramientas de análisis diseñadas ex profeso.
- En “Manuscrito 5 (WSN Tráfico)”, se avanza respecto a los resultados anteriores y se propone un sistema Smart Traffic, para la gestión avanzada y eficiente del tráfico. Para ello la arquitectura se basa en los elementos básicos previamente descritos: u-Clouds, NoT y Gateway. Tal y como se expone en este manuscrito actualmente el escenario de validación que se está desarrollando, se ubica en parquin del Campus rio Ebro de la Universidad de Zaragoza. Se plantea en torno a 5 u-Clouds (3 centradas en monitorizar plazas de parquin y 2 en control de acceso). Incluirán sensores MZTS (Magnetic Zigbee Traffic Sensors), sensores ambientales (estaciones meteorológicas) y elementos visualizadores (enlazándose con el concepto de *Smart Signal* del “Manuscrito 4 (Smart Signal)”); todo ello se encuentra actualmente en desarrollo en el marco del proyecto MovVI.

3.2 TRABAJO FUTURO

Internet de las Cosas es una de las principales líneas de investigación del grupo de investigación en el que se integra el doctorando. En particular, los resultados y conclusiones obtenidas en esta tesis, constituirán la base para las futuras líneas investigadoras:

- En el ámbito de la optimización energética en las Cosas, se puede avanzar en diferentes aspectos:
 - Investigar o mejorar la eficiencia de mecanismos que sean capaces de transformar algún tipo de energía (térmica, radiación, movimiento, química, etc.) en energía eléctrica. Actualmente existe una línea de investigación asociada a la realización de una tesis, que investiga mecanismos de harvesting óptimos de acuerdo a la tecnología de almacenamiento de energía y al ciclo de uso de las Cosas. A partir de las distintas alternativas energéticas, se podrá considerar el diseño de sistemas con múltiples fuentes de energía como entrada y arquitecturas mixtas de almacenamiento (baterías y supercondensadores).
 - Mejorar la eficiencia del dispositivo desde un enfoque múltiple, considerando tanto la arquitectura del dispositivo (selección y tecnología de componentes), el diseño hardware (control activo del consumo de las diferentes etapas del circuito de modo individualizado y segregado) y el firmware (implementación de ciclo de trabajo óptimo y uso de sistemas operativos embebidos frente a los diseños).
- En el ámbito de la interoperabilidad las tareas pasan por avanzar en el concepto de inteligencia distribuida generalizando los resultados y aplicando la solución propuesta en otros escenarios. De modo esquemático se pretende avanzar en las siguientes tareas:
 - Generalización y aplicación del CTP, a otro tipo de dispositivos.
 - Encapsulado de CTP en otros tipos de tecnologías de comunicación (en particular, se ha empezado a trabajar ya con GSM y LORA, por requisitos de un proyecto de investigación activo y por una tesis respectivamente).
 - Investigación en la implementación de inteligencias distribuidas, estudiando mecanismos como: bindings directos y/o condicionados entre dispositivos, con diversos tipos relacionales (uno a uno, uno a varios, o varios a uno), suscripción a notificaciones, escenarios de uso, macros de comandos y su integración en CTP.
 - Armonización y estabilización de CTP para garantizar la interoperabilidad entre las Cosas de distintas NoT en diferentes u-Clouds a través de los respectivos Gateway.
- El desarrollo de soluciones reales, permite mantenerse en la vanguardia de las tecnologías implicadas, algo que es imprescindible para proseguir la investigación en el área de IoT. En

relación con los resultados de la tesis, cabe comentar que actualmente el grupo de investigación participa en los proyectos MovVI (Plan RTC-2014-2425-4 MINECO) y SigueTu (Plan RTC-2015-3359-4 MINECO), ambos estrechamente relacionados con IoT.

- Disponer de mecanismos de comparación entre soluciones va a suponer que las métricas de IoT sean cada vez más necesarias y utilizadas. Por ello, a partir de los trabajos iniciados en esta tesis, se va a continuar con la investigación al respecto, tanto como elemento comparativo, evaluador e incluso como mecanismo de gestión y mantenimiento de un sistema IoT. Las líneas activas al respecto son:
 - Definición y estandarización de nuevas métricas, que pongan de manifiesto de modo simple la calidad de una solución IoT. A partir de la información extraída, se propondrán metodologías de análisis del funcionamiento de IoT ante situaciones externas peculiares (sobrecargas, fallos).
 - Aplicación de las métricas, como elementos para el mantenimiento de los sistemas IoT. En particular, y como respuesta a los requerimientos de los proyectos anteriormente mencionados, a nivel *Gateway*, se están diseñando rutinas de verificación del estado de la red, de auto-mantenimiento y detección de errores en base al análisis histórico de dichas métricas. Análogamente, se manejará el concepto de salud de sistema, como identificador del estado del sistema (generalización a partir de salud de nodo).
 - Diseño de un dispositivo externo que permita realizar análisis forenses del comportamiento (consumo energético, tráfico de datos, etc.) de una Cosa en su propio entorno y en operativa normal. El objetivo es que pueda conectarse de modo mínimamente invasivo y en uso a los dispositivos ya existentes, para analizar su comportamiento en tiempo real durante un periodo de tiempo prolongado.

4 APÉNDICES

4.1 APÉNDICE 1: CARACTERÍSTICAS DE LAS PUBLICACIONES

A continuación se muestran las características de las revistas en las que han sido publicados o enviados los manuscritos que conforman esta Tesis Doctoral. Se especifican los nombres de las revistas así como su índice de impacto (Journal Citation Reports, Web of Knowledge) y el área temática a la que pertenecen. También se detalla el año y la fase de publicación en la que se encuentra cada manuscrito.

Manuscrito 1: Hardware Architecture Design for WSN Runtime Extension

Nombre de la revista: International Journal of Distributed Sensor Networks

ISSN: 1550-1329

Factor Impacto: 0.923; Factor Impacto a los 5 años: 0.735 (JCR 2013)

Áreas temáticas y ranking:

Ciencias de la computación, Sistemas de información: 106/139 Q4

Telecomunicaciones: 58/77 Q4

Estado: Publicado 2013.

Manuscrito 2: Energy-awareness application for the Internet of Things

Nombre de la revista: International Journal of Sensor Networks

ISSN: 1748-1279

Factor Impacto: 0.920; Factor Impacto a los 5 años: 1.053 (JCR 2014)

Áreas temáticas y ranking:

Ciencias de la computación, Sistemas de información: 79/139 Q3

Telecomunicaciones: 43/77 Q3

Estado: Enviado en Noviembre 2015

Manuscrito 3: Protocol and Architecture to Bring Things into Internet of Things

Nombre de la revista: International Journal of Distributed Sensor Networks

ISSN: 1550-1329

Factor Impacto: 0.665; Factor Impacto a los 5 años: 0.601 (JCR 2014)

Áreas temáticas y ranking:

Ciencias de la computación, Sistemas de información: 106/139 Q4

Telecomunicaciones: 58/77 Q4

Estado: Publicado 2014.

Manuscrito 4: Managing Emergency Situations in the Smart City: The Smart Signal

Nombre de la revista: Sensors

ISSN: 1424-8220

Factor Impacto: 2.245; 5-Year Impact Factor: 2.474; (JCR 2014)

Áreas temáticas y ranking: Instrumentos & Instrumentacion

Instrumentos & Instrumentacion: 10/56 Q1

Estado: Publicado 2015.

Manuscrito 5: Wireless Sensor Networks in traffic management systems

Nombre de las actas: Proceedings of the 6th International Conference on Applied Informatics and Computing Theory (AICT'15).ISBN: 978-1-61804-313-9

Área Temática: Informática aplicada, teoría de la computación.

Estado: Publicado 2015.

4.2 APÉNDICE 2: CONTRIBUCIÓN DEL DOCTORANDO Y RENUNCIA DE LOS COAUTORES NO DOCTORES.

D. Roberto Casas Nebra y D. Alvaro Marco Marco, como directores de la presente memoria de Tesis Doctoral realizada por D. Angel Asensio Gimeno para optar al grado de Doctor certifican que,

Todos los coautores de los manuscritos presentados en dicha memoria son Doctores, a excepción de

Dña. Teresa Blanco Bascuas, coautora del “Manuscrito 2”: Energy-Awareness application for the Internet of Things y “Manuscrito 3”: “Managing Emergency Situations in the Smart City: The Smart Signal”.

D. Carlos Trasviña Moreno, coautor del “Manuscrito 2”: Energy-Awareness application for the Internet of Things y “Manuscrito 4”: Wireless Sensor Networks in traffic management systems.

que renuncian a presentar los mismos como parte principal de otra Tesis Doctoral, para lo que firman además el presente documento. A continuación se especifican los coautores Doctores de dichas publicaciones:

D. Roberto Casas Nebra

D. Alvaro Marco Marco

D. Ruben Blasco Marín

Los directores de la Tesis Doctoral:

D. Roberto Casas Nebra

D. Alvaro Marco Marco

Los coautores no Doctores que renuncia a utilización de publicaciones:

Dna. Teresa Blanco Bascuas

D. Carlos Trasviña Moreno

4.3 APÉNDICE 3: PARTICIPACIÓN EN OTROS RESULTADOS.

Las siguientes publicaciones y/o resultados, que se encuentran en el mismo ámbito de investigación que el objeto de la tesis, han sido fruto de colaboraciones durante el desarrollo de la misma:

1. “From the Island of Knowledge to a Shared Understanding: Interdisciplinarity and technology literacy for innovation in Smart Electronic Product Design”. Teresa Blanco, Roberto Casas, Eduardo Manchado-Perez, Ángel Asensio, José M. Lopez-Perez, International Journal of Technology and Design Education (aceptado con cambios menores). Impact Factor (2014): 0.429
2. “Kitchen Activities Recognition Using Inertial Sensors”. Rosella Arpaia, Rubén Blasco, Roberto Casas, David Buldain, Ángel Asensio. Proceedings of the 14th International Conference on Instrumentation, Measurement, Circuits and Systems (IMCAS’15). Salerno, Italy.2015. ISBN: 978-1-61804-313-9
3. “WiFi Sensor Networks: A study of energy consumption”. Carlos A. Trasviña-Moreno, Ángel Asensio, Roberto Casas, Rubén Blasco, Álvaro Marco. International Multi-Conference on Systems, Signals and Devices, 2014.
4. Coautor de patente: “Intelligent system for signaling an emergency in tunnels” Núm. Solicitud: PCT/ES2014/070768 Núm. Fecha de prioridad: 14/10/2013. Fecha de publicacion: 23/04/2015 País de prioridad: España. Empresas que la están explotando: IMPLASER 99 S.L.L
5. Coautor de patente: “Señal con retroiluminación inteligente y autónoma”.Núm. Solicitud: U201230980. Núm. Patente ES1077777. Fecha de prioridad: 25/09/2012. Fecha de concesión: 26/12/2012. País de prioridad: España. Empresas que la están explotando: IMPLASER 99 S.L.L.

4.4 APÉNDICE 4: VISION ECONOMICA Y SOCIAL DE IOT

A continuación se presentan algunos aspectos de la IoT que si bien no son técnicos pueden resultar interesantes tanto para su comprensión como para su contextualización. No se trata de una aportación formal al contenido de la tesis, sino de una exposición y recopilación de información, por lo que su lectura podría obviarse. Se debe indicar que lo expuesto a continuación en ocasiones no está basado en fuentes científico-técnicas, sino en informes de compañías de vigilancia tecnológica, opiniones de expertos y consideraciones personales generadas a partir de la revisión del estado del arte.

4.4.1 CONTEXTO

Junto a la expresión de IoT, han surgido una serie de términos para referirse o bien a conceptos similares, o bien a un subconjunto o superconjunto de la misma. Los límites o diferencias en ocasiones no están completamente definidos y son susceptibles de interpretación. De igual modo, existe una tendencia a hablar de diferentes tipos de Internet para tratar de simplificar y ejemplificar la evolución de la misma, iniciándose con la Internet de los ordenadores, para pasar por las Cosas, las personas, y terminar recientemente en la Internet de todo. A continuación se realiza un repaso a algunos de los términos relacionados.

- *Ambient Intelligence (AmI)*: entorno que, gracias a la tecnología con la que cuenta, es consciente del contexto y de las personas que en él se encuentran siendo capaz de reaccionar y realizar ciertas acciones sobre los mismos. Se asienta sobre los conceptos de computación dispersa y embebida (pervasive computing), ubicua (ubiquitous computing), sensible al contexto (context awareness) y centrada en la persona (human centric interaction). Los elementos que conforma un AmI deben ser, embebidos, conscientes, reactivos y adaptables en cuanto al contexto, y personalizables y anticipar el comportamiento en su relación con las personas. La IoT puede utilizarse como un mecanismo para generar inteligencia ambiental, no obstante el concepto de AmI es bastante anterior al de IoT, pudiendo considerarse como precursor suyo.
- *Wireless Sensor Network (WSN), Wireless Sensor Actuator Network (WSAN)*: Red formada por dispositivos (idealmente pequeños, autónomos y embebidos en el contexto) con capacidad de sensado y/o actuación, computación y comunicación que colaboran entre sí para llevar a cabo una tarea de sensorización o actuación en un entorno. Tradicionalmente puede considerarse que las WSAN han sido el mecanismo físico para desarrollar los AmI, las investigaciones en este ámbito, son de validez en el desarrollo de Cosas.
- *Internet*: concepto tal y como lo conocemos hoy en día.

- *Internet of Computer*: forma de referirse al primer estadio de *Internet*, para incidir en su simplicidad y que se limitaba a interconectar solamente ordenadores.
- *Web of Things (WoT)*: representación y modelado de los objetos del mundo real en *Internet*; por extensión también se refiere a las arquitecturas, interacciones y mecanismos de trabajo con estos modelos.
- *Machine to Machine (M2M)*: concepto genérico que se refiere al intercambio de información entre dos máquinas remotas. Podría contemplarse como una generalización del concepto de internet de los ordenadores. Este término ha sido de amplio uso en el ámbito industrial y en menor medida en el domótico. De algún modo todo desarrollo IoT requiere de mecanismos de comunicación M2M.
- *Industrial Internet of Things (IIoT)*: termino introducido en el año 2000 por la consultora Frost&Sullivan, para hacer referencia a la integración de los procesos productivos complejos con redes de sensores, actuadores y un software transversal. Tradicionalmente los sistemas M2M se han considerado la base de la IIoT. No ha sido hasta recientemente cuando se ha reconsiderado el gran potencial que IoT puede tener sobre la industria.
- *Industry 4.0*: termino promovido por el gobierno alemán, para expresar la idea de lo que podría ser la cuarta revolución industrial (después de la mecanización, electricidad, automatización) que estará caracterizada por una digitalización y fabricación inteligente, por lo que inevitablemente deberá hacer uso de IoT.
- *Internet of Things (IoT)*: tal y como se ha expuesto anteriormente a lo largo del documento.
- *Wearables*: tipo particular de Cosa, con la característica concreta de estar destinada a ser llevada (vestida) por las personas (o animales), para obtener algún tipo de servicio. Actualmente, se está asistiendo a la explosión de los dispositivos *wearables*, siendo el único tipo de Cosa, a la que se le ha asignado una denominación específica.
- *Internet of People (IoP)*: se presenta como la evolución de IoT, bajo la premisa del empoderamiento de las personas, pretendiendo concienciar que la tecnología de IoT debe ser utilizada en última instancia para prestar un servicio a las personas. A veces, este término se concreta aún más y se habla de la *Internet of Me* (principalmente en el ámbito eHealthcare), focalizando en como la tecnología base de IoT puede ayudar a uno mismo.
- *Quantified Self*: tendencia para incorporar tecnología que permita la adquisición, registro y análisis de la vida diaria de las personas. En cierto modo, se relaciona con la idea de Internet of Me, y la capacidad de los *wearables* para extraer datos.
- *Internet of Everything (IoE)*: termino algo difuso, con el que en general se hace referencia a todas las conexiones y agentes que se pueden considerar. Pese a ser prácticamente sinónimo a IoT, en ocasiones IoE se utiliza para aportar un enfoque más centrado en las personas y la sociedad, con intención de recalcar que trasciende a la mera interacción en la que un agente es un dispositivo.

- *Internet of Services (IoS)*: término con el que se pretende reforzar la idea de que el verdadero impacto económico y social de la IoT está en los servicios que genera. Conjunto de servicios generados gracias a la IoT.
- *Internet of Content (IoC)*: menos usado que los anteriores, y con diferentes acepciones. Se utiliza para referirse al conjunto de contenidos o información digital de la red, por lo que en cierto modo, vendría a ser el concepto de Internet tal y como la entendemos pero focalizado en sus contenidos digitales.
- *Cloud Computing*: mecanismo para habilitar acceso ubicuo a internet para compartir recursos de computación. El calificativo *Cloud* acaba utilizándose de forma muy genérica, y hasta ambigua, para acompañar a otros términos, con la intencionalidad de indicar que interviene procesado y/o almacenamiento de forma no local.
- *Fog Computing*: termino de reciente aparición (Stolfo, Salem & Keromytis 2012), con el que se trata de enfatizar que no todos los datos generados por las Cosas de IoT tienen por qué ser subidos a la Nube para ser procesados, sino que también pueden procesarse en la Niebla, es decir, localmente de modo distribuido por las mismas Cosas que los han generado. Así, el termino *Fog Computing*, recupera el concepto de computación ubicua distribuida, pero presentándose como un espacio frontera entre IoT y la Nube.
- *CPS (Cyber Physical Systems)*: Se dice que IoT une elementos del mundo físico e Internet del mundo cibernético, mientras que CPS es el mecanismo de unión entre ambos. Sin embargo por extensión IoT suele tener la misma interpretación. A efectos prácticos, el término CPS es más usado en entornos académicos e IoT en gubernamentales o genéricos.
- *Big Data*: Termino utilizado para referirse a los sistema de generación de gran cantidad de datos, a cualquier conjunto de datos que excede las capacidades normales de un base de datos, y por extensión a las herramientas software implicadas en el análisis de los casos anteriores. IoT permite aumentar drásticamente nuestra capacidad de monitorización y medición del mundo real, por lo que se contempla como el paradigma de *Big Data* por excelencia.

Del mismo modo, que existen un elevado número de conceptos relacionado con IoT, también surgen numerosas apreciaciones incorrectas (White, Gabrie 2014), (Freescale 2013) en relación a ella. Algunas de las más comunes son:

- **Es una novedad.** Si bien actualmente recibe un gran interés, existe una historia previa tras el concepto, tal y como se ha expuesto en la introducción de este documento.
- **Se basa en hacer dispositivos conectados a internet.** No basta con esto, puesto que el objetivo de IoT es la generación de servicios gracias a la interconexión de todas las cosas, entre si y con el entorno.

- **Será una red única y unificada.** IoT al igual que la actual Internet (referida a veces como red de redes), se conformará a través de la interconexión de un gran número de redes, cada una con sus características adaptadas a los requisitos a satisfacer.
- **En breves se dispondrá de un estándar:** Por la propia complejidad del concepto, su transversalidad y generalidad, va a ser improbable la existencia de una única tecnología de interconexión, un único protocolo de interoperabilidad e inclusive una abstracción universal de las Cosas. No obstante, el número de especificaciones se reducirá y en ámbitos específicos será posible cierto nivel de estandarización.
- **Solo importan los datos.** Si bien es cierto que el valor está en los datos, estos son generados por Cosas reales, con sus limitaciones físicas, y si no se es consciente de ello no habrá datos, y por tanto la evolución de IoT fracasará.
- **Un dispositivo solo es IoT, si se conecta directamente a Internet.** Cada dispositivo tiene unas características específicas, lo que restringe sus capacidades de comunicación. Frecuentemente su conexión es a un Gateway, que actuará como adaptador entre redes, y encapsula parte del control y la inteligencia distribuida. Por otro lado, una verdadera Cosa no solo debe ser capaz de conectarse a Internet, sino que idealmente debería hacerlo con cualquier otra Cosa que le rodease, y del modo más directamente posible.
- **IoT es sobre domótica y wearables.** Si bien son los casos más conocidos, y los que por su sencillez se suelen utilizar para divulgar IoT, se estima que otros sectores como el control industrial y el sector primario, serán los más beneficiados de IoT.

4.4.2 SITUACION DE MERCADO DE LA IOT

VALOR AÑADIDO DE LA IOT

La vertiente económica es de vital importancia (Fleisch 2010), puesto que según los expertos, el único modo de conseguir una verdadera IoT, es que los agentes implicados en su desarrollo, consideren que existe un beneficio demostrable. Prácticamente todas las empresas se pueden beneficiar de IoT, tanto aquellas del sector de las TICs como las que a priori pudieran no estar relacionadas con este ámbito. Esto es debido a que IoT aporta beneficios en todas las fases del producto (Mazhelis et al. 2013), desde la fase de diseño, pasando por la de producción, hasta la de explotación o postventa:

- Añade valor al producto (lo hace más “inteligente”) y lo dota de un valor diferencial frente a la competencia. Sin duda es la aplicación más inmediata de IoT. Se debe tener en cuenta su sensata aplicación, por “conectar un producto a Internet o a un Smartphone no va a ser inmediatamente mejor”.

- Facilita operaciones de negocio más inteligentes y decisiones más acertadas y rápidas gracias al acceso a un mayor número de datos e información.
- Mejorar la cadena de suministro (Musa, Gunasekaran & Yusuf 2014):
 - Mejora, simplifica y automatiza el seguimiento de la localización de los diferentes elementos del producto.
 - Mejora la seguridad del dispositivo durante todos los desplazamientos, no solo por la mejor trazabilidad, sino porque se puede incluir información del contexto durante los mismos (por ejemplo si se requiere un transporte en unas condiciones ambientales determinadas).
- Mejorar los procesos productivos. Se puede aplicar en diferentes vertientes, por ejemplo, la monitorización del proceso de producción mediante Smart Metering puede ayudar a mejorar la eficiencia, la gestión en tiempo real del proceso puede permitir una fabricación flexible y adaptable, se puede mejorar la gestión de inventarios, etc.
- Seguimiento del producto (post venta). Analizar el uso del producto, y la interacción del usuario sobre él, permite saber cómo está siendo utilizado, anticipar problemas y/o fallos, analizar causas frecuentes de fallos e incluso obtener información sobre la evolución de los gustos del cliente. Este tipo de acciones ya se está llevando a cabo, así por ejemplo los motores de Rolls Royce se encuentran altamente sensorizados por la propia compañía, y por todos es conocida la recopilación de incidencias por parte de empresas como Microsoft, para mejorar la experiencia del usuario.
- Expandir el modelo de negocio o descubrir nuevos campos de aplicación. John Deere (maquinaria agrícola) desde el año 2012 ha añadido conectividad a sus equipos ofreciendo nuevos servicios como: gestión online de los cultivos, herramientas de apoyo a la decisión (que, donde y cuando cultivar en base a precios, climatología, etc.) y herramientas para la optimización (cálculo de rutas, selección de utillajes), generando así un nuevo negocio. Otro ejemplo muy actual es cómo el uso de dispositivos *wearable*s, está permitiendo que empresas tradicionalmente del sector textil y calzado amplíen sus mercados (con los dispositivos fitness trackers).

Al respecto, los análisis actuales indican que los mercados que se encuentran más demandados en el ámbito de IoT son (IEEE - The Institute 2015):

- Publicidad personalizada a partir de los hábitos de uso extraídos de los dispositivos y servicios que usan los potenciales clientes.
- Información de uso del dispositivo.
- Uso como herramienta del control de costes.
- Sectores que prestan seguridad en las comunicaciones móviles.
- Uso de las capacidades de la IoT para mejorar la seguridad pública.

BENEFICIO ECONÓMICO EN LA IoT: SERVICIOS Y DATOS

La mayoría de los analistas, sugieren que, el verdadero valor económico de IoT se encuentra en los datos (Internet), antes que en los dispositivos (las Cosas). Según esta visión, la rentabilidad económica de IoT se conseguirá principalmente a partir de los beneficios por prestación de servicios por medio de la manipulación de datos (Bosch IoT Lab 2015) y en menor medida a partir de la venta de dispositivos en sí mismos. En el primero de los casos, el beneficio, puede extenderse a lo largo del tiempo y viene definido como un conjunto muy elevado de cuantías económicas en general pequeñas, mientras que, en el segundo caso, se obtiene un beneficio único por cada dispositivo, (la cuantía depende de la naturaleza del dispositivo) como resultado de su venta (Bohli, Sorge & Westhoff 2009). Muchas compañías tradicionalmente del “negocio del silicio” son conscientes de esto y están tratando de añadir valor a sus chips en los múltiples niveles del dispositivo (como sistemas operativos embebidos, seguridad hardware, facilidad de integración, etc.) (Global Semiconductor Alliance, McKinsey & Company 2015).

No obstante, el éxito de IoT no se conseguirá solo con un número elevado de datos, sino desarrollando sistemas y modelos de negocio que den valor a esta información. El valor de la información encerrada en los datos acabará viéndose como cualquier otro recurso o bien, con un valor per se con el que se podrá comerciar y que será variable en el tiempo, y sensible a otros factores. Esto permite anticipar escenarios en los que los datos lleguen a ser bienes financieros con su propia cotización, y con los que, se pueda llegar a especular. El valor de un dato, de modo simplificado, vendrá definido por su utilidad, aunque podrán influir aspectos inflacionistas (estar asociado a movimientos sociales de tendencia), o deflacionista (facilidad de obtención, pérdida de interés). Por ejemplo, considérense los datos de consumo instantáneo de un contador eléctrico, para las compañías distribuidoras pueden tener más interés conocerlos durante el día que por la noche (menor variabilidad junto con mayor capacidad de suministro eléctrico). Los tipos de datos manipulados en la IoT se suelen agrupar en:

- Datos de estado (sensado): estado de una cosa en su sentido más amplio (de la cosa en sí misma y su entorno). Algunos datos de estado, presentan unas características relevantes por lo que son considerados por sí mismos:
 - Localización (y orientación): Muchos servicios son sensibles a la ubicación del destinatario.
 - Datos personalizados: Por datos personalizados (no confundir con personales) se entiende un subconjunto de datos adaptado a las preferencias de consumo de información del agente consumidor de los mismos.
- Datos para la automatización: son usados para el control automático de otros sistemas.
- Datos para la interacción o interface: aquellos especialmente orientados para transmitir alguna información.

Estos tipos de datos, pueden ser manejados conjuntamente, a modo de bucle cerrado para implementar servicios. Considérese el caso de gestión de calefacción de un edificio. Los datos de estado (temperatura y humedad tanto internas como externas) son analizados; un subconjunto personalizado de los mismos, constituirá los datos de interacción con el usuario. El control del confort puede recaer sobre el usuario tras interactuar con estos datos de interacción, aunque el sistema también puede generar una serie de datos para controlar por sí mismo el sistema de calefacción.

Uno de los mayores problemas que está empezando a surgir en IoT es saber cómo utilizar y rentabilizar la información contenida en los datos. Se debe dejar de almacenar datos y comenzar a darles un uso, un mero almacenamiento de la información desembocará en un fracaso. Algunas estimaciones consideran incluso, que solo el 1% de la información actualmente recogida y almacenada por los fabricantes de dispositivos es aprovechada (Manyika et al. 2015). La información recolectada solo es utilizada para detectar anomalías en el sistema y no para otros fines como la optimización, el avance de la tecnología o incluso como feedback de la interacción con el usuario. En ocasiones la visión del flujo de datos en la IoT se reduce a considerar que el objetivo es hacer llegar los mismos hacia un usuario final (equipado, por ejemplo, con toda suerte de wearables a modo de interfaces), o que éste interactúe con su entorno. Pero se estima que en torno al 70% del modelo de negocio de IoT se llevará a cabo en escenario de tipo business-to-business. La explotación económica de los datos no se basará en hacer llegar los mismos a un usuario final, sino al intercambio de los mismos entre empresas.

En cuanto al análisis de la capacidad potencial de los datos (Manyika et al. 2011), las estimaciones resultan sorprendentes, puesto que al parecer, algunas de las mayores oportunidades para los datos de IoT no se encuentra en los entornos esperables como los tecnológicos con alta sensorización. En su lugar el mayor rendimiento se obtendrá en ámbitos como tierras de cultivo, fábricas y otras industrias supuestamente de baja implantación TICs.

REQUISITOS PARA LA ACTIVACIÓN DEL MERCADO DE IoT

Las previsiones y análisis de IoT se suelen hacer desde el enfoque de mercado final, muy focalizado en el servicio que ofrece el producto al usuario, toda vez que este es el mecanismo para la obtención de beneficio económico. Pareciera que en estos análisis, primara la visión de Internet sobre la de las Cosas. Si bien es cierto que el mundo de Internet pone valor en los datos, parece obviarse que para que existan estos datos, son necesarias las Cosas que los generan y que existen otros posibles servicios como control e interacción con el entorno, entre elementos e interfaces. De igual modo pueden surgir servicios de utilidad entre elementos de la IoT, sin que los datos lleguen a alcanzar las capas superiores y por lo tanto sin la manipulación extensiva de los mismos. Una excesiva puesta en valor de los servicios, aparte de obviar la realidad de los dispositivos puede suponer:

- Dejar huérfano el mercado de los dispositivos por considerarse menos atractivo económicamente (mayores inversiones, mayores costes de desarrollo, ventas únicas por dispositivo, etc).
- Estancamiento del avance de la tecnología asociada a los dispositivos. Aunque afortunadamente, la mayor parte de estos avances son aplicables en otros campos (dispositivos electrónicos, almacenamiento energético, etc.), por lo que seguirán existiendo otros alicientes.
- Saturación de servicios y posible deflación del valor de los mismos: Al igual que con las *Apps* en el ámbito de la telefonía móvil, podría ocurrir una sobreproducción de *Apps*, de escasa utilidad o calidad, alentadas por la posibilidad de beneficio rápido. Esta sobreproducción pueden suponer una desincentivación.
- Disminución de la eficiencia general: La necesidad de producir servicios y de ponerlos en mercado lo más rápidamente posible con el menor coste, puede provocar la aparición de servicios no optimizados y grandes consumidores de los recursos del dispositivo que las ejecuta.

Recíprocamente, también es negativo focalizar la atención en las Cosas y poner únicamente en valor los dispositivos. En este caso, al hablar de IoT, se suelen obviar las connotaciones de servicio del termino Internet argumentando que una Cosa pasa a ser habilitadora de IoT, por el mero hecho de dotarla de algún tipo de conectividad. En efecto, este es el primer paso, pero la potencia de IoT pasa por hacer que cualquier Cosa sea interoperable y por los servicios que ella genera. Una excesiva puesta en valor de las Cosas puede suponer:

- Saturación del mercado: Producir Cosas para IoT, sin reflexionar sobre la capacidad de generar servicios de interés a partir de las mismas, puede desencantar a los potenciales clientes y transmitir la sensación temprana de que la IoT es un concepto hueco.
- Obviar las necesidades reales y ofrecer soluciones no eficientes: No contemplar los requisitos del servicio, ni las restricciones del mercado real, y ofrecer soluciones que solo son operativas en contextos muy simplificados.

Por ello, para prevenir esos desajustes, se considera, que el desarrollo de la IoT debe ser un proceso activo y equilibrado desde ambos enfoques: Internet (Servicios o Datos) y Cosas (Dispositivos). El desacoplamiento entre ambas visiones, unida a la necesidad de mantener beneficio económico por parte de los proveedores, lleva a considerar futuras amenazas para la evolución del mercado de IoT:

- Obsolescencia programada: Movida por la necesidad de vender nuevos dispositivos para generar beneficio económico, u ofrecer respuesta a aplicaciones cada vez más exigentes.

- La utilidad de los servicios y su aporte real a la sociedad: Parte del potencial de la IoT, debería utilizarse para mejorar la sociedad, y no como un medio para la generación de nuevos servicios que movilicen un mercado económico, la experiencia demuestra que este tipo de negocios son transitorios y asociados a modas pasajeras.

Por ello, se considera que el mecanismo de creación de beneficio en IoT pasa por la existencia de un amplio ecosistema de empresas (hardware, software, comunicaciones) que puedan operar de modo conjunto y complementario, con total interoperabilidad. Cuando se desarrolla un producto para la IoT el comprador final no es otro desarrollador (no se produce un dispositivo hardware para un desarrollador software), si no que éste hará uso de él, para que un comprador final (externo a ambos) disfrute de un servicio. Los desarrolladores de ambos extremos no son los clientes recíprocos del producto, si no meros creadores del ecosistema. La forma de asegurar el éxito es tener en cuenta que los dispositivos diseñados deben de ser capaces de ofrecer un servicio para los usuarios finales, lo que en muchas ocasiones se consigue a través de que terceros desarrolladores de servicios utilicen el dispositivo. De igual modo, un desarrollador de servicios, conseguirá que su servicio sea tanto más usado, cuantos más desarrolladores de productos puedan orientar su producto hacia ese servicio.

Esta concepción del mercado, parece venir avalada por precedentes de éxito de importantes empresas como Apple o Google en sectores TICs ampliamente relacionados con la IoT. Ambas han desarrollado un producto y creado en torno a él un mercado que permite a terceras empresas generar valor. Apple ofrece un *smartphone* (o más recientemente *smartwatch*) en torno al cual otros generan *Apps*, mientras que Google articula el sistema operativo Android que es integrado por desarrolladores de dispositivos móviles. Recuérdese que esta estrategia se ha mostrado ganadora frente a otros modelos de negocio como los que seguían Nokia/Symbian, Windows Mobile o Blackberry. Recientemente, otras grandes empresas como Amazon (unión de e-commerce con sus subsidiarias como Kindle) e incluso Microsoft están empezando a seguir estrategias similares y desarrollar productos o servicios integrables con otros externos.

Actualmente se apuesta por un futuro panorama en el que un número pequeño de grandes empresas muy especializadas (IBM, CISCO, GE, Telecom, Hosting, etc.) van a desarrollar las infraestructuras base de la IoT, mientras que un mayor número de empresas, tanto establecidas (BOSCH, Nest) como startups van a desarrollar diferentes dispositivos, todo ello será aprovechado por un elevado número de empresas generadoras de servicios. Se espera, que las directrices en el ámbito de los servicios (software, datos) vengan marcadas e incentivadas por las grandes empresas veteranas en este campo (Google y Apple, junto con Microsoft y Amazon tratando de introducirse en el mercado). Pero para que este modelo fructifique tiene que existir una intención real entre todos los agentes de que exista un intercambio de información y comprensión. Aunque cada vez existe más conectividad entre los dispositivos, el hecho de que

estén conectados entre sí, no quiere decir que sepan entenderse; es más, en numerosas ocasiones los fabricantes de esos dispositivos no tienen un interés manifiesto en este intercambio de información

A modo de ejemplo de éxito y actual paradigma de empresa de IoT, cabe presentar el caso de la empresa Nest. Fundada en 2010 por Tony Fadell y Matt Rogers (antiguos ingenieros de Apple) que ofrecía un termostato inteligente. En Enero del 2014 Google adquirió Nest por \$3200 millones, y seis días después, Nest, ya como empresa de Google, adquirió Dropcam por \$555 millones. En Octubre 2014 Nest adquirió Revolv cuya plataforma para la SmartHome, Boulder (hub hardware capaz de soportar diferentes tecnologías y protocolos de comunicación inalámbricos), era una de las más flexibles del mercado. Esta plataforma recibió en su momento buenas críticas, sin embargo su coste \$300 y el hecho de que al ser un hub, parecía que no transmitía al usuario final el espíritu de que las cosas se conectasen directamente a Internet, han hecho que deje de producirse. Nest anuncia como partners suyos a Ivec (Radio despertador inteligente controlado por voz), Life360 (app a modo de microred social entre los miembros de la familia), Pebble (Smart watch), Rachio (aspersores de riego inteligentes) y SNUPI (Sensor Network Utilizing Powerline Infrastructure) Technologies. Actualmente Nest es una empresa de la matriz Alphabet Inc de Google, de 460 empleados, con “tan solo” tres productos básicos: Termostato, Alarma de humo, Cámara de seguridad.

El caso modélico de la empresa Nest, se caracteriza, por haber seguido lo que se han identificado como unas estrategias acertadas, en la consecución de la IoT:

- Tener en cuenta múltiples enfoques: Datos, plataforma y dispositivos.
- Ser consciente de que no se pueden abarcar todos los nichos de mercados, pero es interesante tener algún tipo de presencia en la mayoría. Si no se es capaz de llegar a un nicho, buscar aliados en ese nicho.
- Espíritu integrador y de intercambio de datos. La plataforma “Work with Nest Platform” crea un ecosistema abierto en el que se pueden integrar otros dispositivos.
- Importancia de los datos, como generador de beneficio económico, pero sin menospreciar a los dispositivos.
- Saber identificar clientes, sus necesidades y gustos.
- Pensar en otros desarrolladores que usen sus productos.
- Ser conscientes de la importancia de los propios desarrolladores.
- Ofrecer un servicio al usuario final.

La base para la evolución de cualquier tecnología, acaban siendo sus desarrolladores. En el contexto actual, parece aceptado que los desarrolladores de servicios IoT serán desarrolladores del ámbito web y móvil (Want, Schilit & Jenson 2015). No obstante esto supone el riesgo, de

que estos desarrolladores no sean conscientes de que las Cosas se encuentran restringidas por una serie de factores que impone su propia naturaleza. La futura necesidad de desarrolladores e investigadores en el ámbito de IoT, ya ha sido percibida en el ámbito académico e universitario (Kortuem et al. 2013), en donde se presta especial atención a las consideraciones que deberían tener en cuenta los diseñadores de servicios IoT:

- **Limitaciones en la infraestructura de internet:** Todo dispositivo IoT acaba necesitando un acceso a la Internet, sin embargo actualmente Internet no es ubicua, y el acceso a la misma en algunos casos no es inmediato. El servicio desarrollado debe considerar este hecho, por ejemplo una solución IoT para agricultura, puede dejar de ser rentable si se requiere conectividad GPRS en lugar de WiFi.
- **Conectividad:** A la hora de diseñar el camino de conectividad se debe considerar el punto más conflictivo de la misma. Aunque IoT use como soporte Internet, en el extremo final de la ruta se encuentran los dispositivos que generalmente disponen de recursos limitados (batería, procesamiento y memoria), y sus propios protocolos de comunicación, lo que afecta a la conectividad de los mismos.
- **Diseñar en términos de gran escala:** Los servicios IoT en general se basan en un gran número de dispositivos conectados, con una tasa de simultaneidad alta. Convertir un prototipo de sistema en una implementación real, puede suponer, pasar de manejar 10 dispositivos a cientos de miles en un intervalo de tiempo muy acotado. Si esto no se ha previsto desde el principio, será un fracaso.
- **Concurrencia:** Se suele requerir la capacidad de poder gestionar con cierto grado de simultaneidad un elevado número de dispositivos. El diseño de aplicaciones concurrentes, es una de los puntos más delicados en ciencias de la computación, y que frecuentemente no es tenido en consideración.
- **Optimizar el intercambio de datos:** El beneficio económico, está en la información, y para que esta fluya debe existir una transmisión de datos, que tiene un coste energético (crítico en el dispositivo) y económico (principalmente como peaje por datos). Por ello se debe minimizar el número de bytes intercambiados, con estrategias como: compactar la información con un lenguaje próximo al dispositivo, utilizar mensajes eficientes (alta relación entre bytes de *payload* útil, y bytes totales) y evitar el uso de interacciones inútiles.
- **Distribuir geográficamente los host de los servidores de datos/servicios:** Tanto por cuestiones de seguridad (redundancia), como para mejorar la experiencia del usuario (minimizar tiempos de acceso).
- **Conocer las últimas alternativas que permitan un rápido prototipo del servicio en la fase de evaluación:** Desde lenguajes (Scala, Clojure, o Ruby frente a los clásicos Java, C#), entornos de desarrollo (Google Weave, Brillo) plataformas hardware (Intel Galileo, Raspberry, BeagleBone, Arduino), sistemas de gestión de datos (NoSQL) etc (Hodges et al. 2013).

- **Integrar soluciones existentes:** No volver a diseñar algo que ya es comercial, si no incluirlo en la medida de lo posible.
- Ser consciente de los **gustos** de los **usuarios** y sus **miedos** (privacidad y seguridad)
- **Utilizar planteamientos abiertos:**
 - Herramientas de desarrollo abiertas
 - Facilitar el uso de nuestros desarrollos

MERCADO Y PREVISIONES

Los siguientes datos de mercado (unidades y económicos) se basan en informes (Rivera, van der Meulen 2013), (Lueth 2015), que recogen los análisis de diversas consultoras tecnológicas y/o empresas del sector TIC sobre IoT. Para el año 2020 algunas estimaciones consideran que existirán 50000 millones dispositivos conectados a IoT (CISCO, Ericsson), los más conservadores sitúan la cifra en 18000 millones (IHS Global Insight), mientras que otros toman posiciones intermedias (25000 millones Gartner; 28000 millones IDC y Harbor Research). En general, las predicciones están de acuerdo en que se va a dar un notable incremento, del orden del 14% al 29%, en número de dispositivos frente a las cifras actuales estimadas en el rango de los 14000 millones (CISCO) y los 6000 millones (Global Insight). En todos los estudios se coincide en que para el 2020 habrá más dispositivos IoT que Smartphones, ordenadores y Tablets juntos. Estos dispositivos actualmente rondan los 7000 millones mientras que para el 2020 su número estimado será de 7300 millones. Las predicciones difieren en cuanto al número absoluto de unidades, quizás debido a que las más halagüeñas son llevadas a cabo por empresas directamente relacionadas con los dispositivos IoT.

En cuanto al volumen de negocio directo para las empresas (hardware, software y servicios) proveedoras directas de soluciones IoT, los diferentes incrementos previstos entre el año 2014 y el 2020 son (en billones europeos de dólares): de 2.3 a 7 billones (IDC), de 0.88 a 1.6 billones (VisonGain), de 0.2 a 1 billones (Habor Research), de 0.2 a 0.3 billones (Gartner). Nuevamente se prevé un crecimiento, aunque en función de quien realiza el análisis, el grado de optimismo difiere notablemente. La diferencia en el punto de partida inicial, pone de manifiesto que cada estudio no entiende lo mismo sobre lo que es o no es IoT.

Para el valor económico añadido (el beneficio agregado de todo el negocio derivado de la venta y uso de la IoT) la estimación es todavía más compleja, en tanto en cuanto el concepto añadido es interpretado de distintos modos, se carece de un punto de inicio claro, y los umbrales temporales son distintos. Utilizando como referencia McKinsey e IDTech se estima un impacto positivo en la economía de entre 4 a 12 billones en el 2025 (CISCO llegaría a los 19 billones en el 2035). Por disponer de un umbral de comparación, el PIB español en el año 2014 es 1.4 billones de euros, y según las estimaciones el valor económico añadido de la IoT en el 2025 sería mayor que el PIB alemán (actualmente unos 3.5 billones de dólares).

Como ya se ha comentado, se estima que el potencial económico recae en áreas como la industria, sector primario y la gestión de ciudades. Igualmente llama la atención la dispersión entre el mínimo y máximo en el caso de las aplicaciones del ámbito humano, esto es debido principalmente a la expectación en la evolución de los dispositivos *wearables*, y las posibles implicaciones de estos dispositivos en aspectos de índole legales como normativas médicas y protección de datos.

En relación al procesado de la información, otra perspectiva para cuantificar el impacto que tendrá en el futuro la IoT, es considerar el número de desarrolladores software que se requerirán para crear valor a partir de los datos. Informes de Vision Mobile predicen un paso de los 800000 en 2015 a 4.5 millones en 2020, esto es un crecimiento del 57% anual (Schuermans, Vakulenko 2014). Tras esta necesidad se encuentra el hecho de que la generación de datos es cada vez mayor. Se considera que el 90% de los datos totales generados por la humanidad, se han producido en los últimos dos años (la mayoría generados de modo automatizados por máquinas, sin intervención directa de ninguna persona). Más datos, requieren más profesionales capaces de manipularlos. Análisis de mercado similares, indican que un 53% de los desarrolladores de aplicaciones móviles, actualmente ya trabajan en proyectos relacionados con la IoT. Siendo las dos áreas más activas las relacionadas con las SmartHome (37%), los wearables (35%), pequeñas aplicaciones (20%) y vehículos inteligentes (18%). Sin embargo, resulta notorio comprobar que de estos desarrolladores, en torno a un 30% lo hace como hobby (sin remuneración salarial), un 20% como segundo trabajo, y un 12% como Freelancer (Wilcox, Voskoglou 2015).

De cualquier modo, de lo que no cabe duda, es de la alta actividad en el sector de la IoT, como pone de manifiesto los movimientos M&A (Mergers and Acquisitions) en sectores afines (Liu 2015). Al respecto cabe indicar que en el año 2014 (Yoshida 2015) se ha dado el mayor número de movimientos en los últimos 15 años (60 operaciones con un volumen de \$14.3E9), con un crecimiento notable respecto a años anteriores (19 en 2013, 14 en 2012, 17 en 2011 12 en 2010). Esta intensidad, solo fue superada en el año 2000 en pleno auge de la burbuja “.com”. Durante los años 2013-2014 las compañías más importantes de software y hardware han adquirido a terceras empresas, con objeto de posicionarse mejor en el mercado, así Google ha adquirido 42, Intel 21, Samsung 20, Oracle 19 e IBM 15.

4.4.3 IMPACTO SOCIAL DE LA IOT

Desde una perspectiva centrada en las personas IoT se podría describir como una revolución tecnológica que permitirá disfrutar de mejores o nuevos servicios gracias a la interacción desatendida de las Cosas. De este modo, podemos decir que IoT continua el espíritu de conceptos anteriores como Domótica, AmI, o ambientes asistenciales (AAL), pero generalizándolos en la finalidad y ámbitos, y extendiéndolos en el espacio. Actualmente se teoriza

con que IoT supondrá una revolución en el concepto de sociedad, de modo similar a como Internet supuso un cambio en el concepto de las comunicaciones y la informática (Michahelles, Karpischek & Schmidt 2010).

La previsión de cambio más radical, está relacionada con la capacidad de IoT como herramienta de empoderamiento social (Tei, Gurgen 2014), algo que desarrolla P. H Howard y ha dado en llamar *Pax Technica* (Howard 2015). Predice una sociedad en la que no existe ningún agente dominante, sino un equilibrio en políticas globales, articulado por el pacto entre grandes firmas tecnológicas y los gobiernos. Vaticina una socio-tecnocracia, en la que el gran acceso a la información, la rapidez en la transmisión de la misma, y la imposibilidad de bloqueo favorecerá la aparición de ciudadanos más informados y proactivos, críticos con las formas de poder y control. De igual modo la ciudadanía, dispondrá de mecanismos para ganar visibilidad e interacción con las estructuras de gobierno. No obstante también pone en consideración uno de los grandes problemas de este tipo de sociedades, la privacidad.

Sin duda IoT podrá aportar grandes beneficios, aunque también ha empezado a preocupar sus efectos negativos y las responsabilidades de su uso (Weber 2011). Algunos de ellos son meras suposiciones, como aislamiento social, dependencia tecnológica, brecha tecnológica, derecho de renuncia de uso a esta tecnología, pérdidas de puestos de trabajo etc. Por el contrario, sí se han identificado y comenzado a tener en cuenta dos aspectos concretos, sobre los que ya se está investigando: privacidad y seguridad (Medaglia, Serbanati 2010), (Weber 2010).

PRIVACIDAD

El termino POL (*Pattern Of Life*) hace referencia al conjunto de técnicas para documentar, analizar y comprender el comportamiento de una persona o colectivo de ellas. Esta información puede ser potencialmente usada para comprender el comportamiento pasado (mejorando en el proceso la propia comprensión) e incluso tratar de prever el comportamiento futuro. Tradicionalmente se utilizaba en disciplinas como la antropología o la psicología, pero un artículo en The Guardian en 2013 (Ball 2013) sobre “MARINA” (la base de datos y las herramientas de datos de la NSA) y su capacidad de generación de POLs a partir de los datos de la persona, han convertido este término en popular, comenzando a aplicarse en otros ámbitos.

IoT posibilita un incremento espectacular en la cantidad de datos que se dispone de una persona. Estos van a pasar a ser de hábitos meramente virtuales a datos más físicos y reales de la vida cotidiana. La información, antes puntual, va a abarcar ahora periodos de tiempo mayores de la vida del usuario. Estos datos serán de gran interés principalmente para las empresas y los gobiernos, y la problemática sobre su gestión legal y ética, es uno los puntos más debatidos sobre las implicaciones de la IoT, siendo de hecho uno de los aspectos que más preocupa a los usuarios

(Groopman, Etlinger 2015), (Virkki, Chen 2013). El aspecto de la gestión de datos generados por la IoT presenta varias vertientes:

- Consciencia de ser el origen de los datos. Al respecto, la forma de extraer esta información puede ser:
 - Invasiva (no legal o ilegal) sin consentimiento: Hackeo, el cual constituye un delito.
 - No invasivas sin consentimiento: POLs, monitorización comercial agresiva. Por ejemplo seguimiento de personas en centros comerciales a partir de sus conexiones WiFi, Bluetooth, correladas con su histórico de compras
 - Invasivas con consentimiento. Generalmente se cede parte de la intimidad como contraprestación por un servicio o para colaborar en acciones colectivas.

El caso más preocupante es el de los usuarios que no son conscientes (puesto que la IoT por definición, pretende ser mínimamente invasiva) de que están dejando una huella digital, a partir de la cual se puede obtener importante información, ni de a quien le interesa esa información, ni para que se usa.

- Evitar que recolecten determinados datos, o derecho a la intimidad digital.
- Derecho al olvido o borrado de los datos recolectados.

En esencia, el usuario puede imaginarse que él es dueño de sus propios datos, cuando en realidad acaban en posesión de empresas sobre las que no es consciente (Albrecht, Michael 2013).

Como se pone de manifiesto en un informe remitido en 2013 por la Electronic Privacy Information Center (EPIC) (Electronic Privacy Information Center 2013) a la Federal Trade Commission (FTC), el número de problemas asociados con la privacidad en IoT son numerosos. La FTC consciente de ello ha publicado en Enero de 2015 un informe (FTC Staff Report 2015b) sobre la situación y una guía resumen de buenas prácticas (FTC Staff Report 2015a). A nivel Europeo todavía rige una directiva antigua Directiva 95/46/EC. Aunque en el 2012 se llevó a cabo una propuesta para la protección de datos personales, y la manipulación de los mismos (General Data Protection Regulation, o GDPR a cargo de la European Data Protection Supervisor, o EDPS), que todavía se está negociando, y cuando se apruebe será de obligado cumplimiento inmediato (a diferencia de la directiva que requiere leyes nacionales particulares para ser efectiva). En Septiembre del 2014 un grupo de trabajo establecido por la Directiva 95/46/EC publicó “Opinion 8/2014 on the on Recent Developments on the Internet of Things”.

Aun con este tipo de iniciativas en marcha, se reconoce que puede no ser suficiente, y se ha alertado sobre el abuso que se puede llevar a cabo sobre la parte más desprotegida, los usuarios. Por ello en Julio de 2015, el EDPS declaró su intención de controlar los modelos de negocio

centrados en la recogida y manipulación de datos personales (las denominadas empresas POL, o empresas *Profiling*, como ellas prefieren ser llamadas por parecer más inofensivo).

SEGURIDAD

Se suele distinguir entre dos niveles de seguridad, uno orientado a la prevención (Safety) y otro más centrado en la gestión de la incidencia (Security). Al hablar de seguridad en IoT, generalmente nos estamos refiriendo al primer caso, puesto que al fin y al cabo aún no existe una verdadera IoT en uso normal, sobre la que implementar protocolos de gestión de incidencias. El análisis de la seguridad en IoT se centra principalmente en evitar el robo o modificación (garantizando la autenticidad) de los datos gestionados por IoT, tanto los que están en tránsito (tecnologías de comunicaciones) como los que están en uso (software de procesamiento y bases de datos), evitar suplantaciones de identidad, y accesos a información restringida (Roman, Najera & Lopez 2011). La seguridad de IoT se aborda desde el punto de vista de las tecnologías que la integra, principalmente en aspectos como comunicaciones seguras, encriptación de datos, y prevención de acceso (firewalls tanto hardware como software), (Roman, Zhou & Lopez 2013), (Heer et al. 2011). La investigación en seguridad en las TICs es muy activa puesto que siempre es un objetivo primordial, y en ocasiones no está exenta de polémica. Los usuarios individuales, siempre querrán el máximo nivel de seguridad y privacidad (aunque en ocasiones la declinan de modo más o menos consciente por algún tipo de contraprestación), pero ciertas entidades como empresas y gobiernos, preferirían cierta capacidad de acceso.

Junto a este problema, conforme se implante IoT se intuyen otras cuestiones en el ámbito de la seguridad que deberán ser tratadas, como:

- Protección de la integridad de las infraestructuras: IoT será cada vez más relevante, y se adquirirá una mayor dependencia de la misma, por lo que un cese de servicio (accidental o intencionado) supondrá un problema. IoT se considerará una infraestructura crítica, y se le aplicarán estrategias similares pero particularizadas a las que se utilizan en otros sectores críticos (energético, telecomunicaciones etc).
- Riesgos derivados por el uso de la tecnología: sin apenas contemplar aún, pero cabría preguntarse cómo afectaría un comportamiento incorrecto de un sistema IoT (de modo análogo a como se analizan los efectos de otras tecnologías, siendo el caso más relevante el ámbito de generación energética).

A la vista de estas implicaciones negativas, no son pocos los que tan pronto se empezó a vislumbrar las capacidades de IoT, consideraron sus implicaciones legales (Weber 2009). Como máxima, se debe considerar, que por más segura que sea la tecnología, siempre se podrá encontrar un punto débil, de modo que surgirán ataques a la privacidad y fallos en la seguridad (deliberados o no). Por ello se deberá avanzar no solo en un marco normativo como hasta ahora, sino en una

legislación preventiva para proteger al usuario más débil, y llegado el caso sancionar a los infractores.

5 BIBLIOGRAFIA

- 6LoWPAN 2015, 2015/10/30-last update, *IPv6 over Low power WPAN (6lowpan)*. Available: <http://datatracker.ietf.org/wg/6lowpan/charter/>.
- Abbas, Z. & Yoon, W. 2015, "A Survey on Energy Conserving Mechanisms for the Internet of Things: Wireless Networking Aspects", *Sensors*, vol. 15, no. 10, pp. 24818-24847.
- Albrecht, K. & Michael, K. 2013, "Connected: To Everyone and Everything [Guest Editorial: Special Section on Sensors]", *Technology and Society Magazine, IEEE*, vol. 32, no. 4, pp. 31-34.
- AllSeen 2015, 2015/10/30-last update, *AllSeen Alliance*. Available: <https://allseenalliance.org/>.
- Alvarado, U., Juanicorena, A., Adin, I., Sedano, B., Gutiérrez, I. & Nó, J. 2012, "Energy harvesting technologies for low-power electronics", *Transactions on Emerging Telecommunications Technologies*, vol. 23, no. 8, pp. 728-741.
- Anastasi, G., Conti, M., Di Francesco, M. & Passarella, A. 2009, "Energy conservation in wireless sensor networks: A survey", *Ad hoc networks*, vol. 7, no. 3, pp. 537-568.
- Andreev, S., Galinina, O., Pyattaev, A., Gerasimenko, M., Tirronen, T., Torsner, J., Sachs, J., Dohler, M. & Koucheryavy, Y. 2015, "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap", *Communications Magazine, IEEE*, vol. 53, no. 9, pp. 32-40.
- Apple 2015a, 2015/10/30-last update, *Airplay - Apple*. Available: <https://www.apple.com/airplay/>.
- Apple 2015b, 2015/10/30-last update, *HomeKit - Apple*. Available: <https://developer.apple.com/homekit/>.
- Arabi, K. 2014, *Low power Design Techniques in Mobile Processors*, QUALCOMM Technologies, Inc.
- Asensio, Á, Blasco, R., Marco, Á & Casas, R. 2013, "Hardware architecture design for WSN runtime extension", *International Journal of Distributed Sensor Networks*, vol. 2013.
- Asensio, Á, Marco, Á, Blasco, R. & Casas, R. 2014, "Protocol and Architecture to Bring Things into Internet of Things", *International Journal of Distributed Sensor Networks*, vol. 2014.
- Ashton, K. 2009, "That 'internet of things' thing", *RFID Journal*, vol. 22, no. 7, pp. 97-114.
- Atzori, L., Iera, A. & Morabito, G. 2010, "The internet of things: A survey", *Computer networks*, vol. 54, no. 15, pp. 2787-2805.
- Atzori, L., Iera, A., Morabito, G. & Nitti, M. 2012, "The social internet of things (siot)—when social networks meet the internet of things: Concept, architecture and network characterization", *Computer Networks*, vol. 56, no. 16, pp. 3594-3608.

- Baccelli, E., Hahm, O., Günes, M., Wählisch, M. & Schmidt, T.C. 2013, "Operating Systems for the IoT—Goals, Challenges, and Solutions", *Workshop Interdisciplinaire sur la Sécurité Globale*, .
- Ball, J. 2013, *NSA stores metadata of millions of web users for up to a year, secret files show*.
- Bandyopadhyay, D. & Sen, J. 2011, "Internet of Things: Applications and Challenges in Technology and Standardization", *Wireless Personal Communications*, vol. 58, no. 1, pp. 49-69.
- Bargh, J.A. & McKenna, K.Y. 2004, "The Internet and social life", *Annu.Rev.Psychol.*, vol. 55, pp. 573-590.
- Barnaghi, P., Wang, W., Henson, C. & Taylor, K. 2012, "Semantics for the Internet of Things: early progress and back to the future", *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 8, no. 1, pp. 1-21.
- Baronti, P., Pillai, P., Chook, V.W., Chessa, S., Gotta, A. & Hu, Y.F. 2007, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards", *Computer Communications*, vol. 30, no. 7, pp. 1655-1695.
- Bhuyan, B., Sarma, H.K.D., Sarma, N., Kar, A. & Mall, R. 2010, "Quality of Service (QoS) provisions in wireless sensor networks and related challenges", *Wireless Sensor Network*, vol. 2, no. 11, pp. 861.
- Bi, Z., Da Xu, L. & Wang, C. 2014, "Internet of Things for enterprise systems of modern manufacturing", *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 2, pp. 1537-1546.
- Bohli, J., Sorge, C. & Westhoff, D. 2009, "Initial observations on economics, pricing, and penetration of the internet of things market", *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 2, pp. 50-55.
- Bonino, D., Castellina, E. & Corno, F. 2008, "Dog: An ontology-powered osgi domotic gateway", *2008 20th IEEE International Conference on Tools with Artificial IntelligenceIEEE*, , pp. 157.
- Borges Neto, J.B., Silva, T.H., Assunção, R.M., Mini, R.A. & Loureiro, A.A. 2015, "Sensing in the Collaborative Internet of Things", *Sensors*, vol. 15, no. 3, pp. 6607-6632.
- Bormann, C., Castellani, A.P. & Shelby, Z. 2012, "Coap: An application protocol for billions of tiny internet nodes", *IEEE Internet Computing*, , no. 2, pp. 62-67.
- Bosch IoT Lab 2015, 2015/11/07-last update, *Business Models and the Internet of Things - Bosch IoT Lab @ HSG*.
- Castellani, A.P., Gheda, M., Bui, N., Rossi, M. & Zorzi, M. 2011, "Web Services for the Internet of Things through CoAP and EXI", *Communications Workshops (ICC), 2011 IEEE International Conference onIEEE*, , pp. 1.
- Centenaro, M., Vangelista, L., Zanella, A. & Zorzi, M. 2015, "Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios", *arXiv preprint arXiv:1510.00620*, .

- Chabarek, J., Sommers, J., Barford, P., Estan, C., Tsiang, D. & Wright, S. 2008, "Power awareness in network design and routing", *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, .
- Chang, K., Soong, A., Tseng, M. & Xiang, Z. 2011, "Global wireless machine-to-machine standardization", *IEEE Internet Computing*, , no. 2, pp. 64-69.
- Char, K. 2015, *Internet of Things System Design with Integrated Wireless MCUs*.
- Chen, J., Díaz, M., Llopis, L., Rubio, B. & Troya, J.M. 2011, "A survey on quality of service support in wireless sensor and actor networks: Requirements and challenges in the context of critical infrastructure protection", *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1225-1239.
- Chen, M., Wan, J. & Li, F. 2012, "Machine-to-Machine Communications", *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 6, no. 2, pp. 480-497.
- Contiki 2015, 2015/10/30-last update, *Contiki: The Open Source Operating System for the Internet of Things*. Available: <http://www.contiki-os.org/>.
- Cook, D.J., Augusto, J.C. & Jakkula, V.R. 2009, "Ambient intelligence: Technologies, applications, and opportunities", *Pervasive and Mobile Computing*, vol. 5, no. 4, pp. 277-298.
- Cook, D.J. & Das, S.K. 2012, "Pervasive computing at scale: Transforming the state of the art", *Pervasive and Mobile Computing*, vol. 8, no. 1, pp. 22-35.
- Corson, M.S., Laroia, R., Li, J., Park, V., Richardson, T. & Tsirtsis, G. 2010, "Toward proximity-aware internetworking", *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 26-33.
- Da Xu, L., He, W. & Li, S. 2014, "Internet of Things in industries: A survey", *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 4, pp. 2233-2243.
- Del-Valle-Soto, C., Mex-Perera, C., Orozco-Lugo, A., Lara, M., Galván-Tejada, G.M. & Olmedo, O. 2014, "On the MAC/Network/Energy Performance Evaluation of Wireless Sensor Networks: Contrasting MPH, AODV, DSR and ZTR Routing Protocols", *Sensors*, vol. 14, no. 12, pp. 22811-22847.
- Domingo, M.C. 2012, "An overview of the Internet of Things for people with disabilities", *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 584-596.
- Dondi, D., Bertacchini, A., Brunelli, D., Larcher, L. & Benini, L. 2008, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks", *Industrial Electronics, IEEE Transactions on*, vol. 55, no. 7, pp. 2759-2766.
- Duan, R., Chen, X. & Xing, T. 2011, "A QoS Architecture for IoT", *Internet of Things (iThings/CPSCoM), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*IEEE, , pp. 717.

- EEML 2015, 2015/10/30-last update, *Extended Environments Markup Language*. Available: <http://www.eeml.org/>.
- Electronic Privacy Information Center 2013, *On the Privacy and Security Implications of the Internet of Things_ICM*.
- El-Sayed, H., Mellouk, A., George, L. & Zeadally, S. 2008, "Quality of service models for heterogeneous networks: overview and challenges", *annals of telecommunications-Annales des télécommunications*, vol. 63, no. 11-12, pp. 639-668.
- European Commission 2015a, 2015/10/30-last update, *AIOTI: Alliance for Internet of Things Innovations*. Available: <https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti>.
- European Commission 2015b, 2015/10/30-last update, *Digital Agenda for Europe: A Europe 2020 Initiative*. Available: <https://ec.europa.eu/digital-agenda/en/internet-things>.
- European Commission 2015c, 2015/10/30-last update, *DSM: Digital Single Market*. Available: <http://ec.europa.eu/priorities/digital-single-market/>.
- Fan, Y.J., Yin, Y.H., Da Xu, L., Zeng, Y. & Wu, F. 2014, "IoT-based smart rehabilitation system", *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 2, pp. 1568-1577.
- Farooq, M.O. & Kunz, T. 2011, "Operating systems for wireless sensor networks: A survey", *Sensors*, vol. 11, no. 6, pp. 5900-5930.
- Fernandes, M.A., Matos, S.G., Peres, E., Cunha, C.R., López, J.A., Ferreira, P., Reis, M. & Morais, R. 2013, "A framework for wireless sensor networks management for precision viticulture and agriculture based on IEEE 1451 standard", *Computers and Electronics in Agriculture*, vol. 95, pp. 19-30.
- Fleisch, E. 2010, "What is the internet of things? An economic perspective", *Economics, Management, and Financial Markets*, , no. 2, pp. 125-157.
- Forsström, S., Österberg, P. & Kanter, T. 2012, "Evaluating ubiquitous sensor information sharing on the internet-of-things", *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, , pp. 1454.
- FreeRTOS 2015, 2015/10/30-last update, *FreeRTOS - Market leading RTOS (Real Time Operating System) for embedded systems with Internet of Things extensions*. Available: <http://www.freertos.org/>.
- Freescale 2013, *The Internet of Things: Five Myths and Realities - Freescale*.
- FTC Staff Report 2015a, *Careful connections-building security internet of things_ICM*, Federal Trade Commission.
- FTC Staff Report 2015b, *Internet of Things. Privacy & Security in a Connected World*, Federal Trade Commission.

- Galloway, B. & Hancke, G.P. 2013, "Introduction to Industrial Control Networks", *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 2, pp. 860-880.
- Gao, R.X. & Fan, Z. 2006, "Architectural design of a sensory node controller for optimized energy utilization in sensor networks", *Instrumentation and Measurement, IEEE Transactions on*, vol. 55, no. 2, pp. 415-428.
- Gershenfeld, N. 1999, *When things start to think*, Macmillan.
- Global Semiconductor Alliance & McKinsey & Company 2015, *The Internet of Things: Opportunities and challenges for semiconductor companies*, Global Semiconductor Alliance; McKinsey & Company;.
- Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N. & Razafindralambo, T. 2011, "A survey on facilities for experimental internet of things research", *Communications Magazine, IEEE*, vol. 49, no. 11, pp. 58-67.
- Gomez, C., Oller, J. & Paradells, J. 2012, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology", *Sensors*, vol. 12, no. 9, pp. 11734-11753.
- Google 2015a, 2015/10/30-last update, *Brillo-Google*. Available: <https://developers.google.com/brillo/>.
- Google 2015b, 2015/10/30-last update, *Loon for All – Project Loon – Google*. Available: <http://www.google.com/loon/>.
- Google 2015c, 2015/10/30-last update, *Thead Group - Google*. Available: <http://threadgroup.org/>.
- Groopman, J. & Etlinger, S. 2015, *Consumer Perceptions of Privacy in the Internet of Things: What Brands Can Learn from a Concerned Citizenry*, Altimeter.
- Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. 2013, "Internet of Things (IoT): A vision, architectural elements, and future directions", *Future Generation Computer Systems*, , no. 29, pp. 1645-1660.
- Guinard, D., Trifa, V., Karnouskos, S., Spiess, P. & Savio, D. 2010, "Interacting with the soa-based internet of things: Discovery, query, selection, and on-demand provisioning of web services", *Services Computing, IEEE Transactions on*, vol. 3, no. 3, pp. 223-235.
- Gungor, V.C. & Hancke, G.P. 2009, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches", *Industrial Electronics, IEEE Transactions on*, vol. 56, no. 10, pp. 4258-4265.
- Hamblen, J.O. & van Bekkum, G.M. 2013, "An embedded systems laboratory to support rapid prototyping of robotics and the internet of things", *Education, IEEE Transactions on*, vol. 56, no. 1, pp. 121-128.
- Harb, A. 2011, "Energy harvesting: State-of-the-art", *Renewable Energy*, vol. 36, no. 10, pp. 2641-2654.

- Harrop, P., Harrop, J. & Das, R. 2015, *Internet of Things (IoT): Business Opportunities 2015-2025*, IDTechEx Ltd.
- Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S. & Wehrle, K. 2011, "Security Challenges in the IP-based Internet of Things", *Wireless Personal Communications*, vol. 61, no. 3, pp. 527-542.
- Hempstead, M., Lyons, M.J., Brooks, D. & Wei, G. 2008, "Survey of hardware systems for wireless sensor networks", *Journal of Low Power Electronics*, vol. 4, no. 1, pp. 11-20.
- Higuera Portilla, J.E., Polo Cantero, J. & Gasulla Forner, M. 2010, "A ZigBee wireless sensor network compliant with the IEEE1451 standard", .
- Higuera, J.E. & Polo, J. 2011, "IEEE 1451 standard in 6LoWPAN sensor networks using a compact physical-layer transducer electronic datasheet", *Instrumentation and Measurement, IEEE Transactions on*, vol. 60, no. 8, pp. 2751-2758.
- Hodges, S., Taylor, S., Villar, N., Scott, J., Bial, D. & Fischer, P.T. 2013, "Prototyping Connected Devices for the Internet of Things", *Computer*, vol. 46, no. 2, pp. 26-34.
- Hong, S., Kim, D., Ha, M., Bae, S., Park, S.J., Jung, W. & Kim, J. 2010, "SNAIL: an IP-based wireless sensor network approach to the internet of things", *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 34-42.
- Hong, S.H., Kim, S.H., Kim, G.M. & Kim, H.L. 2014, "Experimental evaluation of BZ-GW (BACnet-ZigBee smart grid gateway) for demand response in buildings", *Energy*, vol. 65, pp. 62-70.
- Howard, P.N. 2015, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*, Yale University Press.
- Huerta, C., Asensio, A., Blanco, T., Blasco, R. & Marco, A. 2015, *Intelligent system for signaling an emergency in tunnels*.
- Huerta, C., Huerta, V., Aparicio, J.I., Pardo, J., Blanco, T., Asensio, Á, Blasco, R., Casas, R. & Marco, Á 2012, *Señal con retroiluminación inteligente y autónoma*.
- IEEE 2015, 2015/10/30-last update, *IEEE P 2413: Standard for an Architectural Framework for the Internet of Things (IoT)*. Available: <http://grouper.ieee.org/groups/2413/>;
- IEEE - The Institute 2015, 2015/11/06-last update, *Special Report: The Internet of Things - IEEE - The Institute*. Available: <http://theinstitute.ieee.org/static/special-report-the-internet-of-things>.
- IIC 2015, 2015/10/30-last update, *Industrial Internet Consortium*. Available: <http://iiconsortium.org/>.
- Ingenu 2015, 2015/10/30-last update, *Ingenu - Dedicated Machine Connectivity for IoT*. Available: <http://www.ingenu.com/>.
- IPSO Alliance 2015, 2015/10/30-last update, *IPSO Alliance*. Available: <http://www.ipso-alliance.org/>.

- Jara, A.J., Zamora, M.A. & Skarmeta, A. 2012, "Global IP: An adaptive and transparent IPv6 integration in the Internet of Things", *Mobile Information Systems*, vol. 8, no. 3, pp. 177-197.
- Jin, J., Gubbi, J., Luo, T. & Palaniswami, M. 2012, "Network architecture and QoS issues in the internet of things for a smart city", *Communications and Information Technologies (ISCIT), 2012 International Symposium on IEEE*, , pp. 956.
- Kaloxylou, A., Eigenmann, R., Teye, F., Politopoulou, Z., Wolfert, S., Shrank, C., Dillinger, M., Lampropoulou, I., Antoniou, E. & Pesonen, L. 2012, "Farm management systems and the Future Internet era", *Computers and Electronics in Agriculture*, vol. 89, pp. 130-144.
- Karimi, K. & Atkinson, G. 2013, "What the Internet of Things (IoT) needs to become a reality", *White Paper, FreeScale and ARM*, .
- Kelly, S.D.T., Suryadevara, N.K. & Mukhopadhyay, S.C. 2013, "Towards the implementation of IoT for environmental condition monitoring in homes", *Sensors Journal, IEEE*, vol. 13, no. 10, pp. 3846-3853.
- Kennedy, J.B. 1926, *An interviews with Tesla*.
- Knight, C., Davidson, J. & Behrens, S. 2008, "Energy options for wireless sensor nodes", *Sensors*, vol. 8, no. 12, pp. 8037-8066.
- Kortuem, G., Bandara, A.K., Smith, N., Richards, M. & Petre, M. 2013, "Educating the Internet-of-Things generation", *Computer*, vol. 46, no. 2, pp. 53-61.
- Kortuem, G., Kawsar, F., Fitton, D. & Sundramoorthy, V. 2010, "Smart objects as building blocks for the internet of things", *Internet Computing, IEEE*, vol. 14, no. 1, pp. 44-51.
- Kranz, M., Holleis, P. & Schmidt, A. 2010, "Embedded interaction: Interacting with the internet of things", *Internet Computing, IEEE*, vol. 14, no. 2, pp. 46-53.
- Kulkarni, R.V., Förster, A. & Venayagamoorthy, G.K. 2011, "Computational intelligence in wireless sensor networks: A survey", *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 1, pp. 68-96.
- Latzer, M. 2009, "Information and communication technology innovations: radical and disruptive?", *New Media & Society*, vol. 11, no. 4, pp. 599-619.
- Lazarescu, M.T. 2013, "Design of a WSN platform for long-term environmental monitoring for IoT applications", *Emerging and Selected Topics in Circuits and Systems, IEEE Journal on*, vol. 3, no. 1, pp. 45-54.
- Lee, K., Sweetser, V., Johannes, J., Eccles, L. & Burch, J. 2007, "IEEE Standard for a Smart Transducer Interface for Sensors and Actuators Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats", *IEEE Instrumentation and Measurement Society*, .
- Li, L., Li, S. & Zhao, S. 2014, "QoS-aware scheduling of services-oriented internet of things", *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 2, pp. 1497-1505.

- Liang, J., Chen, J., Cheng, H. & Tseng, Y. 2013, "An energy-efficient sleep scheduling with QoS consideration in 3GPP LTE-advanced networks for Internet of things", *Emerging and Selected Topics in Circuits and Systems, IEEE Journal on*, vol. 3, no. 1, pp. 13-22.
- Linton, P. & Jaokar, A. 2014, *The Digital World in 2030. What Place for Europe?*, European Internet Foundation, 1000 Brussels, Belgium.
- Liu, J. 2015, "Technology transformation drives record dealmaking in 2014, and sets stage for 'robust' 2015", *EY (Ernst & Young)*, .
- López, T.S., Ranasinghe, D.C., Harrison, M. & McFarlane, D. 2012, "Adding sense to the Internet of Things", *Personal and Ubiquitous Computing*, vol. 16, no. 3, pp. 291-308.
- Lueth, K.L. 2015, "IoT market analysis: Sizing the opportunity", *IoT Analytics*, .
- Lund, D., MacGillivray, C., Turner, V. & Morales, M. 2013, *Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand*, IDC.
- M. Leiner, B., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. & Wolf, S. 2009, "A brief history of the internet", *SIGCOMM Comput. Commun.*, vol. 39, no. 5, pp. 22.
- Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. & Aharon, D. 2015, *Unlocking the potential of the Internet of Things*, McKinsey Global Institute.
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. & Byers, A.H. 2011, "Big data: The next frontier for innovation, competition, and productivity", .
- Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P. & Marrs, A. 2013, *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute.
- Martinez, B., Monton, M., Vilajosana, I. & Prades, J.D. 2015, "The power of models: Modeling power consumption for IoT devices", .
- Mathúna, C.Ó., O'Donnell, T., Martinez-Catala, R.V., Rohan, J. & O'Flynn, B. 2008, "Energy scavenging for long-term deployable wireless sensor networks", *Talanta*, vol. 75, no. 3, pp. 613-623.
- Mattern, F. & Floerkemeier, C. 2010, "From the Internet of Computers to the Internet of Things" in *From active data management to event-based systems and more* Springer, , pp. 242-259.
- Mazhelis, O., Warma, H., Leminen, S., Ahokangas, P., Pussinen, P., Rajahonka, M., Siuruainen, R., Okkonen, H., Shveykovskiy, A. & Myllykoski, J. 2013, "Internet-of-things market, value networks, and business models: State of the art report", *University of JYVÄSKYLÄ, DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS, Technical Reports TR-39*, , pp. 13-14.

- Medaglia, C. & Serbanati, A. 2010, "An Overview of Privacy and Security Issues in the Internet of Things" in , eds. D. Giusto, A. Iera, G. Morabito & L. Atzori, Springer New York, , pp. 389-395.
- Merentitis, A., Kranitis, N., Paschalis, A. & Gizopoulos, D. 2012, "Low energy online self-test of embedded processors in dependable WSN nodes", *Dependable and Secure Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 86-100.
- Michahelles, F., Karpischek, S. & Schmidt, A. 2010, "What Can the Internet of Things Do for the Citizen? Workshop at Pervasive 2010", *Pervasive Computing, IEEE*, vol. 9, no. 4, pp. 102-104.
- Microsoft Reserch 2015, 2015/10/30-last update, *SenseWeb*. Available: <http://research.microsoft.com/en-us/projects/senseweb/>.
- Mitcheson, P.D., Yeatman, E.M., Rao, G.K., Holmes, A.S. & Green, T.C. 2008, "Energy harvesting from human and machine motion for wireless electronic devices", *Proceedings of the IEEE*, vol. 96, no. 9, pp. 1457-1486.
- Morrish, J. 2015, *With 3 billion connections, LPWA will dominate wide area wireless connectivity for M2M by 2023*, Machina Research.
- MQTT 2015, 2015/10/30-last update, *MQTT*. Available: <http://mqtt.org/>.
- Musa, A., Gunasekaran, A. & Yusuf, Y. 2014, "Supply chain product visibility: Methods, systems and impacts", *Expert Systems with Applications*, vol. 41, no. 1, pp. 176-194.
- Näslund, J. 2015, "Low Power Wide Area Solutions:The central role of the Operator and how to fit with other radio technologies", *GSMA's IoT Summit at Mobile World Congress*, July 2015.
- National Communications Systems 2004, *Supervisory Control and Data Acquisition (SCADA) Systems*.
- OASIS 2015, 2015/10/30-last update, *OASIS: Advancing open standards for the information society*. Available: <https://www.oasis-open.org/>.
- OGC 2015, 2015/10/30-last update, *Sensor Model Language (SensorML)*. Available: <http://www.ogcnetwork.net/SensorML>.
- OIC 2015, 2015/10/30-last update, *Open Interconnect Consortium*. Available: <http://openinterconnect.org>.
- Palattella, M.R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L.A., Boggia, G. & Dohler, M. 2013, "Standardized protocol stack for the internet of (important) things", *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 3, pp. 1389-1406.
- Park, T.R. & Lee, M.J. 2008, "Power saving algorithms for wireless sensor networks on IEEE 802.15.4", *Communications Magazine, IEEE*, vol. 46, no. 6, pp. 148-155.

- Paschou, M., Sakkopoulos, E., Sourla, E. & Tsakalidis, A. 2013, "Health Internet of Things: Metrics and methods for efficient data transfer", *Simulation Modelling Practice and Theory*, vol. 34, pp. 186-199.
- Patro, A. & Banerjee, S. 2015, "COAP: a software-defined approach for home WLAN management through an open API", *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 18, no. 3, pp. 32-40.
- Perera, C., Zaslavsky, A., Christen, P. & Georgakopoulos, D. 2014a, "Context Aware Computing for The Internet of Things: A Survey", *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 1, pp. 414-454.
- Perera, C., Zaslavsky, A., Christen, P. & Georgakopoulos, D. 2014b, "Sensing as a service model for smart cities supported by internet of things", *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 1, pp. 81-93.
- Pesovic, U., Jovanovic, Z., Randjic, S. & Markovic, D. 2012, "Benchmarking performance and energy efficiency of microprocessors for wireless sensor network applications", *MIPRO, 2012 Proceedings of the 35th International Convention IEEE*, , pp. 743.
- Petersen, S. & Carlsen, S. 2011, "WirelessHART versus ISA100. 11a: the format war hits the factory floor", *Industrial Electronics Magazine, IEEE*, vol. 5, no. 4, pp. 23-34.
- Pfisterer, D., Römer, K., Bimschas, D., Kleine, O., Mietz, R., Truong, C., Hasemann, H., Kroller, A., Pagel, M. & Hauswirth, M. 2011, "SPITFIRE: toward a semantic web of things", *Communications Magazine, IEEE*, vol. 49, no. 11, pp. 40-48.
- Popovici, E., Magno, M. & Marinkovic, S. 2013, "Power management techniques for Wireless Sensor Networks: A review", , pp. 194.
- Poza-Lujan, J., Posadas-Yagüe, J., Simó-Ten, J., Simarro, R. & Benet, G. 2015, "Distributed Sensor Architecture for Intelligent Control that Supports Quality of Control and Quality of Service", *Sensors*, vol. 15, no. 3, pp. 4700-4733.
- Presser, M., Barnaghi, P.M., Eurich, M. & Villalonga, C. 2009, "The SENSEI project: integrating the physical world with the digital world of the network of the future", *Communications Magazine, IEEE*, vol. 47, no. 4, pp. 1-4.
- Rabaey, J., Ammer, J., Otis, B., Burghardt, F., Chee, Y.H., Pletcher, N., Sheets, M. & Qin, H. 2006, "Ultra-Low-Power Design: The Roadmap to Desappearing Electronics and Ambient Entelligence", *IEEE circuits & devices magazine*, vol. 22, no. 4, pp. 23.
- Rathod, N., Jain, P., Subramanian, R., Yawalkar, S., Sunkenapally, M., Amrutur, B. & Sundaresan, R. 2015, "Performance analysis of wireless devices for a campus-wide IoT network", *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), 2015 13th International Symposium on*, pp. 84.
- Rault, T., Bouabdallah, A. & Challal, Y. 2014, "Energy efficiency in wireless sensor networks: A top-down survey", *Computer Networks*, vol. 67, pp. 104-122.

- Razzaque, M.A., Javadi, S.S., Coulibaly, Y. & Hira, M.T. 2014, "QoS-Aware Error Recovery in Wireless Body Sensor Networks Using Adaptive Network Coding", *Sensors*, vol. 15, no. 1, pp. 440-464.
- Remagnino, P. & Foresti, G.L. 2005, "Ambient intelligence: A new multidisciplinary paradigm", *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 35, no. 1, pp. 1-6.
- Riot 2015, 2015/10/30-last update, *The friendly Operating System for the Internet of Things - Riot*. Available: <http://www.riot-os.org/>.
- Rivera, J. & van der Meulen, R. 2013, "Gartner Says The Internet Of Things Installed Base will grow to 26 Billion Units By 2020", *Stamford, conn., December*, vol. 12.
- Rodrigues, J.J. & Neves, P.A. 2010, "A survey on IP-Based wireless sensor network solutions", *International Journal of Communication Systems*, vol. 23, no. 8, pp. 963-981.
- Roman, R., Najera, P. & Lopez, J. 2011, "Securing the Internet of Things", *Computer*, vol. 44, no. 9, pp. 51-58.
- Roman, R., Zhou, J. & Lopez, J. 2013, "On the features and challenges of security and privacy in distributed internet of things", *Computer Networks*, vol. 57, no. 10, pp. 2266-2279.
- Saint-Andre, P. 2011, "Extensible messaging and presence protocol (XMPP): Core", .
- Salvadori, F., De Campos, M., Sausen, P.S., De Camargo, R.F., Gehrke, C., Rech, C., Spohn, M.A. & Oliveira, A.C. 2009, "Monitoring in industrial systems using wireless sensor network with dynamic power management", *Instrumentation and Measurement, IEEE Transactions on*, vol. 58, no. 9, pp. 3104-3111.
- Sardini, E. & Serpelloni, M. 2011, "Self-powered wireless sensor for air temperature and velocity measurements with energy harvesting capability", *Instrumentation and Measurement, IEEE Transactions on*, vol. 60, no. 5, pp. 1838-1844.
- Schuermans, S. & Vakulenko, M. 2014, "IoT: Breaking Free from Internet and Things. How Communities and data will shape teh future of IoT in ways we can't imagine.", *VisionMobile Ltd.*, .
- Sehgal, A., Perelman, V., Kuryla, S. & Schönwälder, J. 2012, "Management of resource constrained devices in the internet of things", *Communications Magazine, IEEE*, vol. 50, no. 12, pp. 144-149.
- Semtech 2015, 2015/10/30-last update, *Semtech Internet of Things (IoT)*. Available: <http://www.semtech.com/wireless-rf/iot.html>.
- Sendra, S., Lloret, J., García, M. & Toledo, J.F. 2011, "Power Saving and Energy Optimization Techniques for Wireless Sensor Networks", *Journal of communications*, vol. 6, no. 6, pp. 439-459.

- Sharma, A., Shinghal, K., Srivastava, N. & Singh, R. 2011, "Energy management for wireless sensor network nodes", *International Journal of Advances in Engineering & Technology*, vol. 1, no. 1, pp. 7-13.
- Shearer, F. 2011, *Power management in mobile devices*, Newnes.
- Shelby, Z. 2012, "Constrained RESTful Environments (CoRE) Link Format", .
- Singh, D., Tripathi, G. & Jara, A.J. 2014, "A survey of Internet-of-Things: Future vision, architecture, challenges and services", *Internet of Things (WF-IoT), 2014 IEEE World Forum on IEEE*, , pp. 287.
- Song, E.Y. & Lee, K. 2008a, "Understanding IEEE 1451-Networked smart transducer interface standard-What is a smart transducer?", *Instrumentation & Measurement Magazine, IEEE*, vol. 11, no. 2, pp. 11-17.
- Song, E.Y. & Lee, K.B. 2008b, "STWS: A unified web service for IEEE 1451 smart transducers", *Instrumentation and Measurement, IEEE Transactions on*, vol. 57, no. 8, pp. 1749-1756.
- Specification, Z. 2008, "ZigBee cluster library specification", *053474r17*, .
- Stankovic, J. 2014, "Research directions for the internet of things", *Internet of Things Journal, IEEE*, vol. 1, no. 1, pp. 3-9.
- Stolfo, S.J., Salem, M.B. & Keromytis, A.D. 2012, "Fog computing: Mitigating insider data theft attacks in the cloud", *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on IEEE*, , pp. 125.
- Sudevalayam, S. & Kulkarni, P. 2011, "Energy harvesting sensor nodes: Survey and implications", *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 3, pp. 443-461.
- Swan, M. 2012, "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0", *Journal of Sensor and Actuator Networks*, , pp. 217-253.
- Synapse Wireless 2015, 2015/10/30-last update, *Synapse Wireless (Synapse Wireless- Proven Solutions for the Internet of Things | Machine-to-Machine (M2M))*.
- Szarka, G.D., Stark, B.H. & Burrow, S.G. 2012, "Review of power conditioning for kinetic energy harvesting systems", *Power Electronics, IEEE Transactions on*, vol. 27, no. 2, pp. 803-815.
- Tan, Y.K. & Panda, S.K. 2011, "Energy harvesting from hybrid indoor ambient light and thermal energy sources for enhanced performance of wireless sensor nodes", *Industrial Electronics, IEEE Transactions on*, vol. 58, no. 9, pp. 4424-4435.
- Tei, K. & Gurgun, L. 2014, "ClouT: Cloud of things for empowering the citizen clout in smart cities", *Internet of Things (WF-IoT), 2014 IEEE World Forum on IEEE*, , pp. 369.
- Thiesse, F. & Michahelles, F. 2010, "Smart Objects as Building Blocks for the Internet of Things", *IEEE Internet Computing*, , pp. 44-51.

- Thread Group 2015, <http://www.synapse-wireless.com/>-last update, *Thread Group*. Available: <http://threadgroup.org/About.aspx>.
- TinyOS 2015, 2015/10/30-last update, *TinyOS Home Page*. Available: <http://www.tinyos.net/>.
- Tozlu, S., Senel, M., Mao, W. & Keshavarzian, A. 2012, "Wi-Fi enabled sensors for internet of things: A practical approach", *Communications Magazine, IEEE*, vol. 50, no. 6, pp. 134-143.
- Trappeniers, L., Feki, M.A., Kawsar, F. & Boussard, M. 2013, "The internet of things: the next technological revolution", *Computer*, vol. 46, no. 2, pp. 0024-25.
- Uthra, R.A. & Raja, S. 2012, "QoS routing in wireless sensor networks—A survey", *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, pp. 9.
- Virkki, J. & Chen, L. 2013, "Personal Perspectives: Individual Privacy in the IOT", .
- Vlacheas, P., Giaffreda, R., Stavroulaki, V., Kelaidonis, D., Foteinos, V., Poullos, G., Demestichas, P., Somov, A., Biswas, A.R. & Moessner, K. 2013, "Enabling smart cities through a cognitive management framework for the internet of things", *Communications Magazine, IEEE*, vol. 51, no. 6, pp. 102-111.
- Vullers, R., van Schaijk, R., Doms, I., Van Hoof, C. & Mertens, R. 2009, "Micropower energy harvesting", *Solid-State Electronics*, vol. 53, no. 7, pp. 684-693.
- Wang, H., Xi, M., Liu, J. & Chen, C. 2013a, "Transmitting IPv6 packets over Bluetooth low energy based on BlueZ", *Advanced Communication Technology (ICACT), 2013 15th International Conference on IEEE*, , pp. 72.
- Wang, W., De, S., Cassar, G. & Moessner, K. 2013b, "Knowledge representation in the internet of things: semantic modelling and its applications", *Automatika—Journal for Control, Measurement, Electronics, Computing and Communications*, vol. 54, no. 4.
- Wang, W., De, S., Toenjes, R., Reetz, E. & Moessner, K. 2012, "A comprehensive ontology for knowledge representation in the internet of things", *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on IEEE*, , pp. 1793.
- Want, R., Schilit, B.N. & Jenson, S. 2015, "Enabling the Internet of Things", *Computer*, , no. 1, pp. 28-35.
- Weber, R.H. 2011, "Accountability in the Internet of Things", *Computer Law & Security Review*, vol. 27, no. 2, pp. 133-138.
- Weber, R.H. 2010, "Internet of Things – New security and privacy challenges", *Computer Law & Security Review*, vol. 26, no. 1, pp. 23-30.
- Weber, R.H. 2009, "Internet of things – Need for a new legal environment?", *Computer Law & Security Review*, vol. 25, no. 6, pp. 522-527.

- Weiser, M. 1991, "The computer for the 21st century", *Scientific American*, vol. 265, no. 3, pp. 94-104.
- Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M. & Borriello, G. 2009, "Building the internet of things using RFID: the RFID ecosystem experience", *Internet Computing, IEEE*, vol. 13, no. 3, pp. 48-55.
- Wemlinger, Z. & Holder, L. 2011, "The cose ontology: Bringing the semantic web to smart environments" in *Toward Useful Services for Elderly and People with Disabilities* Springer, , pp. 205-209.
- West, J. & Gallagher, S. 2006, "Challenges of open innovation: the paradox of firm investment in open-source software", *R&D Management*, vol. 36, no. 3, pp. 319-331.
- White, P. & Gabriele, C. 2014, "Beware the Five Myths of the Internet of Things - Rethink Technology Research Ltd", *White Paper, FreeScale and ARM*, .
- Whitmore, A., Agarwal, A. & Da Xu, L. 2014, "The Internet of Things—A survey of topics and trends", *Information Systems Frontiers*, vol. 17, no. 2, pp. 261-274.
- Wilcox, M. & Voskoglou, C. 2015, *State of the Developer Nation Q1 2015.
Tracking the latest mobile & IoT developer trends across platforms, regions, and revenues.*
- Winter, T. 2012, "RPL: IPv6 routing protocol for low-power and lossy networks", .
- Xia, F. 2008, "QoS challenges and opportunities in wireless sensor/actuator networks", *Sensors*, vol. 8, no. 2, pp. 1099-1110.
- Xiong, N., Wu, Z., Huang, Y. & Xu, D. 2014, "Analyzing Comprehensive QoS with Security Constraints for Services Composition Applications in Wireless Sensor Networks", *Sensors*, vol. 14, no. 12, pp. 22706-22736.
- Xiong, X., Zheng, K., Xu, R., Xiang, W. & Chatzimisios, P. 2015, "Low power wide area machine-to-machine networks: key techniques and prototype", *Communications Magazine, IEEE*, vol. 53, no. 9, pp. 64-71.
- Xu Li, Rongxing Lu, Xiaohui Liang, Xuemin Shen, Jiming Chen & Xiaodong Lin 2011, "Smart community: an internet of things application", *Communications Magazine, IEEE*, vol. 49, no. 11, pp. 68-75.
- Yang, L., Yang, S. & Plotnick, L. 2013, "How the internet of things technology enhances emergency response operations", *Technological Forecasting and Social Change*, vol. 80, no. 9, pp. 1854-1867.
- Yang, Y., Liu, Q., Gao, Z., Qiu, X. & Meng, L. 2015, "Data Fault Detection in Medical Sensor Networks", *Sensors*, vol. 15, no. 3, pp. 6066-6090.
- Yoshida, J. 2015, "Top 2014 Acquisitions that Advanced the Internet of Things", *EETimes*, [Online], .

- Yu, J., Feng, L., Jia, L., Gu, X. & Yu, D. 2014, "A Local Energy Consumption Prediction-Based Clustering Protocol for Wireless Sensor Networks", *Sensors*, vol. 14, no. 12, pp. 23017-23040.
- Yu, P., Qinghua, L. & Xiyuan, P. 2010, "The design of low-power wireless sensor node", *Instrumentation and Measurement Technology Conference (I2MTC), 2010 IEEE*, , pp. 917.
- Zhengguo Sheng, Shusen Yang, Yifan Yu, Vasilakos, A., McCann, J. & Kin Leung 2013, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities", *Wireless Communications, IEEE*, vol. 20, no. 6, pp. 91-98.
- Zorzi, M., Gluhak, A., Lange, S. & Bassi, A. 2010, "From today's intranet of things to a future internet of things: a wireless-and mobility-related view", *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 44-51.
- Zuehlke, D. 2010, "SmartFactory—Towards a factory-of-things", *Annual Reviews in Control*, vol. 34, no. 1, pp. 129-138.