UNIVERSIDAD DE MURCIA

Facultad de Informática, Departamento de
Ingeniería de la Información y las Comunicaciones

PROPUESTA DE UNA ARQUITECTURA DE RED BASADA EN INTERNET DE LAS COSAS PARA LA INTEGRACIÓN UBICUA DE ENTORNOS CLÍNICOS CON SOPORTE ESCALABLE A LA SEGURIDAD Y LA MOVILIDAD

Tesis Doctoral

Presentada por:
D. Antonio Jesús Jara Valera

Supervisada por:
Prof. Dr. D. Antonio Fernando Skarmeta Gómez
Dr. D. Miguel Angel Zamora Izquierdo

Murcia, 2013

D. Juan Antonio Sánchez Laguna, Profesor Titular de Universidad del Área de Ciencia de la Computación e Inteligencia Artificial y presidente de la Comisión Académica del Programa de Doctorado en Informática de la Universidad de Murcia, INFORMA:

Que la Tesis Doctoral titulada *"PROPUESTA DE UNA ARQUITECTURA DE RED BASADA EN INTERNET DE LAS COSAS PARA LA INTEGRACIÓN UBICUA DE ENTORNOS CLÍNICOS CON SOPORTE ESCALABLE A LA SEGURIDAD Y LA MOVILIDAD"*, ha sido realizada por D. Antonio Jesús Jara Valera, bajo la inmediata dirección y supervisión de D. Antonio Fernando Skarmeta Gómez y D. Miguel Angel Zamora Izquierdo, y que la Comisión Académica ha dado su conformidad para que sea presentada ante la Comisión General de Doctorado.

En Murcia, a 8 de Abril de 2013

D. Juan Antonio Sánchez Laguna

D. Antonio Fernando Skarmeta Gómez, Catedrático de Universidad del Área de Ingeniería Telemática en el Departamento de Ingeniería de la Información y las Comunicaciones de la Universidad de Murcia, AUTORIZA:

La presentación de la Tesis Doctoral titulada *"PROPUESTA DE UNA ARQUITECTURA DE RED BASADA EN INTERNET DE LAS COSAS PARA LA INTEGRACIÓN UBICUA DE ENTORNOS CLÍNICOS CON SOPORTE ESCALABLE A LA SEGURIDAD Y LA MOVILIDAD"*, realizada por D. Antonio Jesús Jara Valera, bajo mi inmediata dirección y supervisión, en el Departamento de Ingeniería de la Información y las Comunicaciones, y que presenta para la obtención del grado de Doctor Europeo por la Universidad de Murcia.

En Murcia, a 8 de Abril de 2013

D. Antonio Fernando Skarmeta Gómez

D. Miguel Angel Zamora Izquierdo, Profesor Titular de Universidad del Área de Tecnología Electrónica en el Departamento de Ingeniería de la Información y las Comunicaciones de la Universidad de Murcia, AUTORIZA:

La presentación de la Tesis Doctoral titulada *"PROPUESTA DE UNA ARQUITECTURA DE RED BASADA EN INTERNET DE LAS COSAS PARA LA INTEGRACIÓN UBICUA DE ENTORNOS CLÍNICOS CON SOPORTE ESCALABLE A LA SEGURIDAD Y LA MOVILIDAD"*, realizada por D. Antonio Jesús Jara Valera, bajo mi inmediata dirección y supervisión, en el Departamento de Ingeniería de la Información y las Comunicaciones, y que presenta para la obtención del grado de Doctor Europeo por la Universidad de Murcia.

En Murcia, a 8 de Abril de 2013

D. Miguel Angel Zamora Izquierdo

A mis padres por darme siempre libertad para elegir,
a la vez que me orientaban por el buen camino.

Agradecimientos

Este es el fruto de una vida vinculado a la informática, durante la cual he tenido la gran oportunidad de encontrar muchos amigos y personas a las que les debo mi más sincero agradecimiento.

Durante los primeros años fue muy especial poder pasar largas horas en la pequeña tienda de informática de mi pueblo, donde con toda la paciencia del mundo, Pedro siempre tenía la capacidad de enseñarme y dejarme mirar como aplicaba la magia de la informática.

Después de aquellos años, creo que siempre tuve claro que quería estudiar informática, y desde el primer dia que fui a echar la matricula conocí al que durante una gran aventura de cinco años seria mi compañero de prácticas y sobre todo amigo. Siempre le tendré que agradecer a Fran por enseñarme el valor del compañerismo.

De la carrera, no me puedo olvidar del que siempre he considero en cierta medida mi hermano mayor, Javi. Él siempre ha sabido darme un buen consejo, confiar en mi y sobre todo ser un gran ejemplo de la definición de buena persona. Y a Alberto, un amigo de los de verdad, de esos que siempre están ahí.

De la carrera debo agradecer a todos los profesores que me apoyaron en los inicios cuando empece a mostrar interés por la investigación, ofreciendome la oportunidad de integrarme en los grupos como alumno interno.

Este contacto inicial con la investigación me llevó hasta la personas que a día de hoy son mis mentores, directores y sin duda las personas que más han influido en mi realización como profesional. No me puedo imaginar haber logrado esto con otros dos directores que no hubiesen sido Antonio y Miguel Ángel.

En particular, a Miguel Angel le debo agradecer su capacidad para escucharme, ayudarme a diferenciar entre lo valioso y lo superfluo, y sobre todo por su esfuerzo por convertir a un joven con simplemente ideas en un investigador con rigor.

A Antonio le debo agradecer su criterio, claridad, objetividad y sobre todo por ser un ejemplo a seguir sin igual. Siempre ha sabido darme la cantidad necesaria de libertad para poder ir creciendo profesionalmente, a la vez que sabía ser estricto y dirigirme para ayudarme a focalizar y mejorar. Le debo agradecer la oportunidad de permitirme aprender en un grupo de investigación donde la excelencia era la base, donde siempre se espera más de uno, y en el que nunca es suficiente. Todos ellos han sido los ingredientes necesarios para que con trabajo, ilusión y más trabajo siga avanzando en el camino a través del cual llegar a ser un profesional digno de ser llamado investigador.

Además a Antonio y Miguel Angel les debo agradecer la oportunidad que me dieron durante esta tesis de poder establecer un pequeño laboratorio sobre tecnologias de comunicación en entornos clínicos (CliTech), el cual gracias al trabajo y apoyo de grandes amigos, personas y sobre todo cada día más grandes profesionales, como son Alberto, Miguel, Pablo, David, Jesús Alberto y José Felix, hemos logrado hacer realidad nuestras pequeñas ideas y grandes sueños con la formula de la amistad, el buen rollo y sobre todo una gran dosis de compañerimo.

También tengo que agradecer a otros profesores que me han ayudado durante el desarrollo de la tesis como Benito Úbeda que siempre ha tenido un hueco para explicarme teoría de señales, y Leandro Marín por iniciarme en el mundo de la criptografía, sabiendome mostrar la belleza de los números y hacerme imaginar un mundo donde las dimensiones no están limitadas a 3 ni en el que 2 más 2 eran siempre 4, sobre todo si estabamos trabajando en aritmética modular. Además de ellos que sin duda también han sido grandes mentores durante el camino de esta tesis, no debo olvidar al resto de mis compañeros que me han acompañado durante los años del doctorado como Agustin, Alfredo, José López, Manolo, José Santa, Antonio Moragón, Pedro M. Juliá, Rafa y Cristina con los que he tenido el mejor entorno de trabajo que jamás podria haber imaginado.

Gracias a mi familia, a mi abuelo por haber sido el motivo y la luz de gran parte de este trabajo. A mis padres por enseñarme desde que nací el valor del trabajo, el esfuerzo, el respeto, y sobre todo el afan por la auto-superación. Y sobre todo gracias a Diana por llegar cuando más la necesitaba y hacer que todo esto tenga sentido.

Gracias a todos los que han confiado en mi y han hecho que esto sea posible

UNIVERSITY OF MURCIA

Faculty of Computer Science, Department of
Information and Communications Engineering

COMMUNICATION ARCHITECTURE FOR CLINICAL ENVIRONMENTS BASED ON THE INTERNET OF THINGS TO SUPPORT SCALABLE SECURITY AND MOBILITY

PhD Thesis

Author:
D. Antonio Jesús Jara Valera

Thesis advisors:
Prof. Dr. D. Antonio Fernando Skarmeta Gómez
Dr. D. Miguel Angel Zamora Izquierdo

Murcia, 2013

To my parents by always giving me freedom to do my own choices,
while they guided me in the right direction.

Contents

List of Figures

Resumen

La cantidad de dispositivos electrónicos, electrométricos, ordenadores, dispositivos personal y en general cosas que están conectadas a Internet está creciendo exponencialmente. Este crecimiento está llevando a una concepción de Internet: .[El] Internet de las cosas".

Los ecosistemas basados en Internet de las cosas están compuestos de dispositivos, llamados objetos inteligentes, con prestaciones muy reducidas en cuanto a capacidad de memoria, batería, cálculo y de comunicación. Además de esos objetos inteligentes, el Internet de las cosas está compuesto de etiquetas y códigos de identificación que permiten la identificación única y escala global de un determinado objeto o cosa.

Para lograr estos ecosistemas, son múltiples las tecnologías disponibles que nos permiten el desarrollo de este tipo de objetos y recursos.

En primer lugar para el desarrollo de objetos inteligentes encontramos tecnologías como *6LoWPAN* para redes de sensores (basadas en IEEE 802.15.4), *Bluetooth Low Energy* (IEEE 802.15.1) para redes de área personal, *WiFi Low Power* (IEEE 802.11) para redes de área local, y finalmente tecnologías celulares como *Long Term Evolution – Advanced (LTE-A)* para comunicaciones máquina a máquina en redes de área extendida.

En segundo lugar, para la identificación de objetos o cosas, las tecnologías más extendidas históricamente son los códigos de barras. El código de barras permite llevar a cabo una identificación siempre de un recurso a nivel de identificador de tipo de producto y fabricante. Como una evolución al código de barras, han aparecido los códigos bidimensionales, los cuales ofrecen una mayor capacidad, permitiendo así almacenar más información acerca del producto etiquetado y la creación de un identificador único a nivel de producto en concreto (*item*), así como su enlace con Internet a través de la inclusión de enlaces de Internet (URL - *Universal Resource Locators*). Además de las técnicas impresas, la gran revolución de las tecnologías para la identificación de objetos o cosas durante los últimos 20 años ha venido de la mano de la tecnología para identificación por radiofrecuencia (RFID - *Radio Frequency Identification*). RFID ofrece múltiples ventajas a las tecnologías de identificación impresas, tales como permitir que múltiples objetos o cosas puedan ser identificados simultáneamente, poder identificar objetos que no se encuentra en la línea de visión, y un mayor almacenamiento sin que tenga ello que afectar a un incremento en el tamaño de la etiqueta. Como una evolución de RFID llegó la integración de RFID en los móviles para identificación de objetos dentro de un campo cercano (NFC - Near

Field Communication). NFC ofrece las capacidades de RFID integradas en el móvil, y además incorpora funcionalidades extra como el establecimiento de comunicaciones entre dos dispositivos (P2P - *Peer-to-Peer*).

Finalmente, otras tecnologías y dispositivos existentes en el Internet actual también están siendo participativos de los ecosistemas formados por Internet de las cosas, un claro ejemplo de este tipo de dispositivos son los teléfonos inteligentes (*smart phones*), tabletas, portátiles, tecnologías industriales, electrodomésticos y dispositivos domóticos.

Esta nueva concepción de extender Internet a todas las cosas es posible gracias a la nueva versión del protocolo de Internet: IPv6.

IPv6 extiende el espacio de direccionamiento para ser capaz de albergar todas las cosas que están siendo conectadas a Internet.

IPv6 ha sido diseñado para ofrecer comunicaciones seguras a los usuarios, así como movilidad a todos los dispositivos utilizados por ese usuario. De esa manera, el usuario puede estar conectado en cualquier momento y desde cualquier lugar de una forma segura.

Esas características de IPv6 es lo que ha hecho posible pensar en conectar todos los objetos y crear un Internet de las cosas.

El objetivo de Internet de las cosas es la integración y unificación de todas las comunicaciones, sistemas y dispositivos disponibles a nuestro alrededor.

De esa manera los sistemas y dispositivos son capacidades de poder comunicarse con otros sistemas y dispositivos con el objetivo de poder ofrecer una nueva generación de servicios potenciados por las capacidades de la comunicación y computación ubicua.

IPv6 ha sido considerada la tecnología más adecuada para el Internet de las cosas, ya que ofrece una alta escalabilidad, flexibilidad, está muy extendido, Internet ha sido probado de una forma intensiva durante los últimos años, está disponible en todas partes, es abierto y ofrece conectividad entre cualquier par de dispositivos conectados a Internet.

Por esa razón, esta tesis ha propuesto mecanismos y protocolos para direccionar cualquier tipo de objeto, recurso o cosa con una dirección IPv6 con el objetivo de alcanzar una red basada en IPv6 que integre múltiples tecnologías en un espacio de direccionamiento común.

En concreto, para el direccionamiento de recursos sin capacidad de ser programados, o recursos que utilizan pilas de comunicaciones de antaño, se ha propuesto la tecnología denominada IPv6 Addressing Proxy, y para los dispositivos emergentes con capacidad de ser programados y con pilas de comunicación noveles tales como Bluetooth Low Energy se ha desarrollado el protocolo GLoWBAL IPv6.

GLoWBAL IPv6 ofrece una integración ligera de las partes que ponen la cabecera de IPv6 para comunicaciones globales, ofreciendo un mayor rendimiento y menor sobrecarga que 6LoWPAN. A través de la conexión de todos los dispositivos a IPv6, Internet de las cosas se está convirtiendo en ecosistema más ubicuo y móvil.

Una vez que todas las cosas son accesibles a través de una dirección IPv6, podría ser considerado que también podrían ser beneficiadas con todos los protocolos desarrollos

en torno a IPv6, es decir, protocolos para movilidad en IPv6 como MIPv6 y protocolos para soportar la seguridad en IPv6 como IPSec. Sin embargo, no es posible que todas las cosas integradas en el Internet de las cosas puedan ser asociadas con protocolos diseñados para dispositivos con mayores prestaciones.

Los dispositivos de Internet de las cosas, los mencionados objetos inteligentes presentan altas restricciones de recursos y energía. Los protocolos desarrollados para dispositivos tales como ordenadores personales y servidores requieren una gran cantidad de señalización y una serie de requisitos que no pueden ser satisfechos por los objetos inteligentes debido a sus restricciones. Por ejemplo, supongamos una red de sensores basada en 6LoWPAN sobre la tecnología IEEE 802.15.4, un sensor 6LoWPAN puede quedarse sin batería y perder la conectividad con la red. Además, tienen restricciones del tamaño de paquete y presentan unas estrategias muy agresivas para reservar energía, como estar la mayor parte del tiempo durmiendo, es decir inaccesible. Este tipo de características introduce retardos para la recepción de mensajes, que no han sido considerados para la mayoría de los protocolos, por lo que puede ocurrir que el protocolo considere que el nodo no está disponible o que ha expirado el tiempo para responder como una consecuencia de no tener en cuenta que hay dispositivos en la red que presentan un mayor tiempo de respuesta con el objetivo de lograr la mayor autonomía posible a nivel de energía.

Sin embargo, el soporte a la movilidad y la seguridad continua siendo requerido para el Internet de las cosas.

Soporte a la movilidad es interesante para el Internet de las cosas dado que soluciones consciente de la movilidad aumenten la conectividad y mejoran la adaptación a cambios de la localización del objeto, así como cambios en la infraestructura,

Internet de las cosas está haciendo posible una nueva generación de entornos dinámicos en lugares como entornos clínicos y ciudades inteligentes.

Entornos dinámicos requieren acceso ubicuo a Internet, cambio de red sin cortes, flexibilidad para el acceso a las redes disponibles, e interoperabilidad con la infraestructura existente. Estas características son retos para el Internet de las cosas.

Esta tesis presenta un análisis de los requisitos, características deseables, soluciones existentes y propuesta para, por un lado, detección de la dirección del movimiento para radios basadas en IEEE 802.15.4 para el cambio rápido de red, y por otro lado, una versión eficiente y ligera del protocolo MIPv6.

Además, también se ha considerado una solución alternativa para arquitecturas de red diferentes a la red IPv6, como es la arquitectura optimizada para la integración de la heterogeneidad y soporte de la movilidad a través de la separación del identificador de la cosa en la red de su localizador (HIMALIS - Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation). Este tipo de arquitecturas basadas en la separación del identificador de red de su localizador soportan de forma nativa la movilidad.

Ambas soluciones presentan un rendimiento y solución adecuada, pero sin embargo la solución basada en una versión eficiente y ligera de Mobile IPv6 merece ser remarcada, dado que una de las mayores consideraciones para el Internet de las cosas es ofrecer

soluciones que sean escalables y que puedan ser interoperable en múltiples dominios y entornos, es decir que no estén limitados a una arquitectura o dominio muy concreto y poco extendido.

La integración e interoperabilidad con la infraestructura existente es uno de los requisitos más importantes para el soporte de la movilidad, ya que los objetos móviles necesitan la capacidad de conectarse a otras redes compatibles con ellos cuando se mueven y dejan de poder conectarse a su red inicial. Por lo tanto, soluciones que son compatibles con las redes, puntos de acceso y enrutadores existentes cobran una mayor relevancia.

Por lo que el hecho de que las soluciones se bases en IPv6 van a ser una consideración clave para el existo de Internet de las cosas en términos de interoperabilidad, aceptación e integración.

Además de la movilidad, la seguridad también es clave para el Internet de las cosas. El vinculo entre el mundo físico y el mundo cibernético o virtual que crea el Internet de las cosas trae riesgos para la seguridad y la privacidad.

Ahora, una vulnerabilidad no está limitada a las fronteras del ordenador, sino que también puede afectar a la red eléctrica, los sistemas de control de accesos, e incluso a cuando cruzar o no la calle en una ciudad inteligente.

Por esas razones, seguridad y privacidad son consideradas como los mayores retos del Internet de las cosas. Seguridad ha sido ya considerado un gran asunto en esta nueva era de la sociedad digital y múltiples soluciones ya existen, por esa razón para del camino ya está hecho, el reto es como extender ahora esas soluciones a los dispositivos que forman el Internet de las cosas.

La seguridad también es un requisito para el soporte a la movilidad, dado que la movilidad ofrece los mecanismos necesarios para re-direccionar tráfico a una nueva dirección que clame ser el nodo que se ha movido. Por lo tanto, movilidad presenta un conjunto de vulnerabilidades tales como ataque de un intruso interceptando la comunicación (*man-in-the-middle*), suplantación de la identidad, e integridad de datos. Para evitar esas vulnerabilidad, se requiere la autenticación del nodo que se ha movido y una asociación de confianza segura entre la red original del nodo que se ha movido y el nodo.

Este trabajo ha diseñado, desarrollado y evaluado un protocolo escalable y seguro para la arquitectura HIMALIS, denominado HIMALISSEC. Además, IPSec ha sido evaluado para el enfoque basado en IPv6.

El soporte de IPSec es obligatorio con IPv6 y con MIPv6. En MIPv6 es usado para proteger las comunicaciones entre el nodo que se ha movilidad y su red original. IPSec presenta dos retos, en primer lugar, la librería criptográfica a ser utilizada, y en seguridad lugar la sobrecarga que supone IPSec para las comunicaciones. Para el primer reto se ha llevado a cabo una optimización de la implementación de la criptografía de curva elíptica para soportar criptografía asimétrica en dispositivos con capacidad restringida. Por otro lado, para el segundo reto, una integración de una versión ligera de IPSec ha sido analizada.

La evolución descrita del Internet de las cosas hacia un Internet más ubicuo y móvil está influenciando en múltiples áreas de aplicación y sectores de mercado.

En particular, para el sector médico está haciendo posible la salud personalizada.

La salud personalizada ofrece la monitorización y soporte a los pacientes en su propio entorno, es decir, el despliegue de sistemas para la monitorización remota y móvil.

Las capacidades de esas soluciones son altamente extendidas. Por ejemplo, la monitorización de constantes vitales de forma continúa para la detección temprana de enfermedades a partir de la detección de anomalías, la correlación de diferentes señales vitales, y su evaluación a lo largo del tiempo con ciencias tales como la cronobiología pueden ser aplicadas.

Una arquitecta de comunicaciones basada en Internet de las cosas para entornos clínicos ha sido diseñada y desarrollada con el soporte a los mencionados elementos clave como son la seguridad y la movilidad.

Esta arquitectura hace posible la monitorización continúa y remota de señales vitales. Además, introduce innovaciones tecnológicas para conectar los dispositivos clínicos con Internet. Esta conexión con Internet permite la monitorización y supervisión por centros remotos, así como desde dispositivos personales como tabletas.

Seguridad es el mayor requisito en entornos clínicos, dado que una vulnerabilidad en la seguridad afecta directamente a la salud del paciente y su privacidad. Por ejemplo, un ataque de denegación de servicio podría para la monitorización continua de un paciente, que en caso de presentar alguna anomalía no sería notificada. Otro ejemplo, es que un intruso suplantase la identidad de un paciente e indicase que se encuentra bien cuando en realidad el paciente puede estar sufriendo algún problema. Por lo tanto, el soporte a la seguridad para prevenir ataques como los descritos es necesario para hacer factible el desarrollo de estos mercados en el sector de la salud.

El soporte a la movilidad en entornos clínicos es requerido dado que los dispositivos clínicos pueden ser conectados a través de tecnologías inalámbricas. Movilidad ofrece una mayor calidad de experiencia para los usuarios, dado que pueden moverse con mayor libertad mientas están siendo monitorizados a través de dispositivos portables o vestibles. El soporte a la movilidad también permite extender la cobertura a todo el hospital y ofrecer tolerancia a fallos, dado que en caso de dejar de estar operativo un punto de acceso, el algoritmo de movilidad haría que se adaptase automáticamente al siguiente punto de acceso más cercano.

Por lo tanto, entornos clínicos es uno de los escenarios donde el soporte para la movilidad en el Internet de las cosas explota su capacidad. Por un lado, la tolerancia a fallos influye directamente en el soporte a la vida, y por otro lado, la monitorización continúa influye a la calidad de los datos disponibles, los cuales pueden ser utilizados para diagnostico en tiempo real con algoritmos basados en cronobiología, o con el algoritmo desarrollado en esta tesis denominado YOAPY.

YOAPY ofrece un protocolo ligero para el nivel de aplicación para sensores tales como electrocardiograma, capnografo, y valores discretos de glucómetros, sensores de

temperatura, tensión arterial, etc. YOAPY ha sido diseñado para ofrecer un eficiente, seguro y escalable integración de los sensores desplegados en el entorno del paciente.

Las capacidades para proveer monitorización continua, conectividad ubicua, conectividad, integración de un gran rango de dispositivos, y soporte para la seguridad y la privacidad han sido evaluadas sobre la arquitectura de comunicación propuesta.

La arquitectura de comunicación para entornos clínicos ha sido evaluada exhaustivamente para enfermedades crónicas como la diabetes, la monitorización continúa de enfermedades cardiacas, adherencia y seguimiento del tratamiento, y finalmente en el contexto del proyecto AIRE, para paciente con problemas respiratorios.

Internet de las cosas es considerado uno de los mayores avances en las tecnologías de la comunicación durante los últimos años. Internet de las cosas ofrece los pilares para el desarrollo de aplicaciones y servicios colaborativos. Muchos trabajos se están llevando a cabo para la aplicación del Internet de las cosas en otra áreas como automatización de edificios, transportes, y en particular para entornos clínicos.

El potencial del Internet de las cosas para entornos clínicos ha sido presentado en esta tesis, presentando las capacidades de las tecnologías de identificación para la identificación de medicamentos, y las capacidades de comunicación para ofrecer terapia de forma ubicua y móvil, a través de las capacidades de conectividad inalámbrica y movilidad para dispositivos personales y objetivos inteligentes, permitiendo la recolección de datos en cualquier lugar y en cualquier momento.

Esta tesis ha desarrollado los componentes clave para explotar la capacidades descrita de Internet de las cosas in construir una arquitectura de comunicación para ofrecer salud personalizada en el entorno del paciente. A este respecto, la arquitectura busca la extensión de esos entornos personales a entornos clínicos. De esa manera una ***integración de entornos clínico de forma ubicua, segura y móvil*** es alcanzada.

Abstract

The number of things that are connected to the Internet is growing exponentially. This has led to defining a new conception of Internet, the commonly called Internet of Things.

Internet of Things ecosystems are composed, on the one hand, of so called smart objects, i.e., tiny and highly constrained physical devices in terms of memory capacity, computation capability, energy autonomy, and communication capabilities. On the other hand, Internet of Things is made up of identification tags and codes that allow identifying a specific thing in a unique and global way.

Several technologies are enabling these types of things.

First, dealing with smart objects we can find technologies such as 6LoWPAN for Wireless Sensor Networks (IEEE 802.15.4), Bluetooth Low Energy (IEEE 802.15.1) for Wireless Personal Area Networks, WiFi Low Power (IEEE 802.11) for Wireless Local Area Networks, and finally Long Term Evolution – Advanced (LTE-A) for machine to machine communications in Wide Area Networks.

Second, for the identification of things the most extended technologies are barcode for the simple identification of a resource (e.g., product identifier), Quick Response (QR) or matrix barcodes for the extended identification of a resource (e.g., plain text and Universal Resource Locators (URLs)), Radio Frequency Identification (RFID) for the digital identification of resources with capabilities for multiple resource identification, identification out of line of sight, and extended identification capability. Finally, Near Field Communication (NFC) for the digital identification of resources through personal devices such as smart phones, and the establishment of peer-to-peer (P2P) communications.

Finally, other existing Internet technologies and devices such as smart phones, tablets, laptops, industrial technologies, appliances, and building automation are also considered part of the Internet of Things.

This new conception of extending Internet to everything is feasible thanks to the new version of the Internet Protocol (IPv6). IPv6 spreads the addressing space in order to support all the emerging Internet-enabled devices.

IPv6 has been designed to provide secure communications to users and mobility for all devices attached to the user; thereby users can always be connected.

IPv6 features are what have made it possible to think about connecting all the objects and to build the Internet of Things.

The objective of the Internet of Things is the integration and unification of all communications systems that surround us. Hence, the systems can get a total control and access to the other systems in order to provide ubiquitous communication and computing with the purpose of defining a new generation of services.

IPv6 is considered the most suitable technology for the Internet of Things, since it offers scalability, flexibility, tested, extended, ubiquitous, open, and end-to-end connectivity.

For that reason, this thesis has proposed specific mechanisms enabling an IPv6 address for each one of the things; ranging from identification tags and legacy technologies to the mentioned emerging technologies to build smart objects. Thereby, the integration of multi-technology networks in a common all-IP network is reached.

For the first nature of devices, i.e., identification tags, and legacy technologies from building automation and industrial control the IPv6 Addressing Proxy technology has been proposed, and for the second nature of devices, i.e., emerging technologies such as Bluetooth Low Energy and to offer a lightweight integration of IPv6 header for global communications an optimization of 6LoWPAN, denominated GLoWBAL IPv6 has been proposed.

Thereby, Internet of Things is moving towards a more ubiquitous and mobile Internet-powered ecosystem.

Once all the things are IPv6 addressable, we can consider that they are also empowered with all the IP protocols, i.e., protocol for mobility such as MIPv6 and security such as IPSec. However, it is not feasible for all the things and resources integrated into the Internet of Things ecosystems to be associated with protocols designed with the considerations of devices with higher capabilities.

Internet of Things devices, the so-called smart objects, are energy and resource constrained, host based protocols require most of the signaling on end nodes and because the design features of the Internet of Things networks were not considered in the design issues of the host based protocols. For example, considering a network with the technology 6LoWPAN over IEEE 802.15.4, a 6LoWPAN node may run out of energy causing a fault in the network, this has restriction in size packets and this presents aggressive techniques to conserve energy by using of sleep schedules with long sleep periods, they just wake up to receive IPv6 signaling messages, this feature introduces delays in the reception of messages because they are not attended until that the node wakes up. Therefore, these delays, power restrictions, and packet size restrictions are not considered in the current IPv6 protocols.

Nevertheless, Mobility management and security continue being required for the Internet of Things.

Mobility management is a desired feature for the emerging Internet of Things. Mobility-aware solutions increase the connectivity and enhance adaptability to changes of location and infrastructure. Internet of Things is enabling a new generation of dynamic ecosystems in environments such as smart cities and hospitals.

Dynamic ecosystems require ubiquitous access to Internet, seamless handover,

flexible roaming policies, and an interoperable mobility protocol with the existing Internet infrastructure. These features are challenges for Internet of Things devices due to their constraints. This thesis presents an analysis of the requirements, desirable features, existing solutions and proposes, on the one hand, detection of movement direction for IEEE 802.15.4 radios to offer a fast handover, and on the other hand, an efficient solution for constrained environments compatible with IPv6-existing protocols, i.e., Mobile IPv6.

In addition to the IPv6-related solution for mobility, a solution for alternative networking architectures such as ID/Locator Split architectures has been proposed. This alternative solution is based on the HIMALIS architecture (HIMALIS means Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation), which have been designed to support mobility in a native way.

Both solutions present a proper performance and solution, but the solution based on Lightweight Mobile IPv6 needs to be highlighted, since one of the major considerations for the Internet of Things is to offer scalable and inter-domain solutions that are not limited to specific application domains or infrastructure.

The integration and interoperability with the existing infrastructure is one of main requirements for mobility management in dynamic ecosystems, since mobile nodes require the capability to use other networks during roaming. For that reason, it is important to offer a highly compatible solution with available access points, routers and networks.

IPv6-based solutions are key enablers for the success of the Internet of Things interoperability, acceptance and integration.

In addition to the mobility, security is a high requirement for the Internet of Things. This close relationship between the cybernetic and the physical world enabled by the Internet of Things carries with it vulnerabilities in terms of security and privacy. Since vulnerability is now not simply limited to the hardware of our computer. as well it is also able to reach our energy systems, physical access control systems, and even when we cross the street in a smart city.

For that reason, security and privacy are considered as one of the major issues for the Internet of Things. Security is already considered as a big issue in the current digital society, and several solutions and mechanism have been built. Therefore, part of the path is already paved, the major challenge now is how to extend these mechanisms to the Internet of Things devices, define new mechanisms more focused on identity and privacy, and the most important challenge, how to make them scalable and feasible for a future with billions of devices interconnected to Internet.

Security is also an inherent requirement for the mobility management, since this offers the capability to redirect traffic to a new address and claim the identity of a node. Therefore, mobility opens a high number of vulnerabilities for the man in the middle attacks, identity supplantation, and data integrity. In order to avoid these vulnerabilities, we require the authentication of the mobile node such as is carried out in Mobile IPv6 with the trust relationship between the mobile node and its home agent.

This work has designed, developed and evaluated a scalable secure protocol for

the HIMALIS architecture, denominated HIMALISEC. In addition, IPSec has been evaluated for IPv6-based approach.

IPSec support is mandatory with IPv6 and used by the MIPv6 protocols. MIPv6 is used to protect the communications between the mobile node and the home agent.

IPSec presents two challenges, first, the cryptosuite which is to be used, and second the overhead from the IPSec headers. For the first issues, an optimization of the Elliptic Curve Cryptography to offer a suitable asymmetric key cryptography for constrained devices is presented, regarding the overhead; a lightweight integration of IPSec is analyzed.

The described evolution from the Internet of Things towards a ubiquitous and mobile Internet is having influence in several application areas and market sectors.

Particularly, in the healthcare sector it is making feasible the development of a more personalized care.

Personalized healthcare offers monitoring/coaching of the patients in their own environments, i.e., the deployment of personalized remote monitoring systems (telecare) and mobile health solutions.

The capabilities of these solutions are highly extended. For example, continuous vital sign monitoring for the early detection of medical conditions through the measuring of anomalies, the co-relation of the different vital signs, and their evolution over time with health sciences such as chronobiology are applied.

A communication architecture based on the Internet of Things for clinical environments has been designed and developed with the described enablers of support for security and mobility.

This architecture makes continuous and remote vital sign monitoring feasible. It introduces technological innovations for empowering health monitors and patient devices with internet capabilities. It allows patient monitoring and supervision from remote fixed centers, and personal mobile platforms such as tablets.

Security is a major requirement in clinical environments, since the security vulnerabilities directly affect patient health and privacy. For example, first, a Deny of Service (DoS) attack could stop continuous vital sign monitoring of a critical patient, consequently in case of anomalies, there would be no alarm. Second, impersonation attack could reply false information from a patient, e.g. informing that he is not in danger when he is. Therefore, the need for security mechanisms is clear to prevent the attacks and to minimize the adverse effects of such attacks in the healthcare market.

Since clinical devices can be connected through wireless technologies mobility management in clinical environments is required. Mobility offers highly valuable features such as higher quality of experiences for the patients since it allows the patients to move freely, continuous monitoring through portable and wearable sensors, extends the coverage to all the hospital, and finally there is a higher fault tolerance since the mobility management allows the connection to adapt dynamically to different access points. Therefore, clinical environments are one of the main scenarios where

the mobility for the internet of things applications shows off these capabilities. On the one hand, fault tolerance influences directly in life support. On the other hand, continuous monitoring influences the quantity of data available which is required for real-time diagnostic with algorithms such as chronobiology-based algorithms and the developed protocol YOAPY.

YOAPY offers a novel protocol for the application layer. This is a lightweight application protocol for electrocardiogram, capnography; and discrete values from sensors such as glucometer, blood pressure, and temperature. It has been designed and developed for an efficient, secure, and scalable integration of the sensors deployed in the personal environment of the patient.

The capabilities to provide continuous monitoring, ubiquitous connectivity, extended device integration, reliability, and support for security and privacy have been evaluated continuously in the proposed architecture.

The communication architecture for clinical environments has been exhaustively evaluated for chronic disease management such as diabetes, continuous monitoring of cardiovascular diseases, drug adherence, and finally in the framework of the AIRE project, for patients with breathing problems.

Internet of Things is considered one of the major communication advances in recent years, since it offers the basis for the development of cooperative services and applications. Extensive research using this concept in different areas, such as building automation, Intelligent Transport Systems, and in particular for healthcare, is being carried out. For example, its potential for mobile health applications has been reported in this thesis, showing its potential identification capacities for drug identification, and its communication capabilities in offering ubiquitous therapy by providing wireless and mobility capabilities for personal devices and smart objects, in addition to allowing the collection of data anytime and anywhere.

This thesis has developed the enablers to exploit the aforementioned Internet of Things capabilities in order to build a communication architecture for personalized healthcare in the patient environment. To this end, this architecture goal is the extension of those environments towards a clinical environment. Thereby, ***Ubiquitous, Secure and Mobile Integration of Clinical Environments*** is reached.

Chapter 1

Introduction

I. Motivation

Motivation for the Internet of Things

The Internet of Things (IoT) [2], or Machine-to-Machine (M2M), is one of the main drivers for the evolution of the Internet towards the Future Internet.

Nowadays, sensors, actuators and devices (so-called things), are connected to the Internet through gateways and platforms such as Supervisory Control and Data Acquisition platforms (SCADAs), panels, and brokers. These gateways and platforms break the end-to-end connection with the Internet. For that reason, this initial approach is defined as an Intranet of Things [3].

The Intranet of Things is being extended to smart things [4] with a higher scalability, pervasiveness, and integration into the Internet Core. This extension is leading to reach a real IoT, where things are first class citizens in the Internet, and they do not need to relay any more on a gateway, middleware, proxy, or broker.

IoT requires both an architecture and products that allow for the extension of Internet technologies, in order to reach a Future Internet of Things, Services and People.

IoT drives towards integrating everything into the Internet Core. This integration is motivated by the market wish to have all processes remotely accessible through an uniform medium – while at the same time understanding that re-engineering an infrastructure to allow this for each application independently would be prohibitively costly and time-consuming. Moreover, the current evolution from uniform mass markets, to personalized ones, where the customization and user-specified adaptation is a requirement, makes the sort of uniform infrastructure found in the Internet, imperative. This allows many components to be re-used, and services to be shared, with correspondingly huge economies of scale and shortened implementation times.

IoT fills the gap between the needs arising from the evolution of the market, information, users, and things, by moving all of them to a common framework, the Internet. This is different from the current approach in such applications, where they are based on stand-alone and monolithic solutions designed for a narrow or *-stovepiped-* application domain. Users now require more flexibility and freedom. Offering a common framework allows choice among the available manufacturers, suppliers, service providers, delivery options, and payment services. While this obviates the need for standalone or proprietary solutions, it also requires a high level of integration.

IoT allows communication among very heterogeneous devices connected via a very wide range of networks through the Internet infrastructure. IoT devices and resources are any kind of device connected to Internet, from existing devices, such as servers, laptops, and personal computers, to emerging devices such as smart phones, smart meters, sensors, identification readers, and appliances.

In addition to the physical devices, IoT is also enriched with the cybernetic resources and Web-based technologies. For that purpose, IoT is enabled with interfaces based on Web Services such as RESTFul architecture and the novel protocol for Constrained devices Applications Protocol (CoAP) [5]. These interfaces enable the seamless

integration of the IoT resources with information systems, management systems, and the humans. Reaching thereby a universal and ubiquitous integration among human networks (i.e., society), appliance networks, sensor networks, machine networks, and, in definitive, everything networks.

Due to the above mentioned potential, IoT is receiving a lot of attention from the academia and industry sectors.

IoT offers several advantages and new capabilities for a wide range of application areas. For example, nowadays IoT is finding applications for the development of *Smart Cities*, starting with the *Smart Grid*, *Smart Lighting* and transport with new services such as *Smart Parking* and the *Bicycle Sharing System* [6] for building sustainable and efficiently smart ecosystems.

The application of the IoT is not limited to high scale deployments such as the locations in Smart Cities, elsewhere it can also be considered for consumer electronics, vehicular communications, industrial control, building automation, logistic, retail, marketing, and healthcare.

Motivation for the Internet of Things in clinical environments

The evolution of sensing and measuring systems lead towards more ubiquitous and mobile solutions. The International Telecommunication Union-Telecommunications (ITU-T) Technology Watch report concludes that the healthcare sector was moving towards a more personalized healthcare with remote monitoring and tele-healthcare support [7].

Personalized healthcare offers monitoring/coaching of patients in their own environments, i.e., the deployment of personalized remote monitoring systems (tele-care) and mobile health solutions. These systems and solutions require more intelligent physiological sensors, characterized by low power consumption, and with advanced wireless communications.

Advances in wireless communications are required in order to connect the physiological sensors deployed in the patient environment, and in wearable wireless body area networks.

The capabilities of these solutions are highly extended. For example, continuous vital sign monitoring for the early warnings of medical conditions through the detection of anomalies, the co-relation of the different vital signs, and its evolution over time with sciences such as chronobiology, can be used [8].

The advance in wireless communications from the perspective of the IoT is also impacting on the application and new capabilities for remote monitoring and mobile health (mHealth). The potential of the IoT for clinical environments and mobile health (mHealth) applications was initially reported in [9] - a work carried out in conjunction with Prof. Robert Istepanian, recognized as the first scientist to coin the concept mHealth.

IoT offers capabilities for, on the one hand, the identification of objects, drugs, equipment tracking and patients/staff through technologies such as Radio Frequency Identification (RFID), and on the other hand, for communication and ubiquitous access to information, such as wireless personal devices, embedded systems and smart objects.

These technologies make it feasible to identify, sense, locate, and connect all the people, machines, devices and things available in clinical environments.

An example of an application where these capabilities are exploited for chronic disease management was presented in the solution for diabetic patients, found in [10], Ambient Assisted Living [11] and wireless healthcare networks [12].

The main motivation for applying the IoT in clinical environments is to build the interconnection framework for personalized healthcare that links the patient's environment with conventional healthcare environments such as hospitals. IoT offers the potential to offer ubiquitous healthcare, because it is not only oriented towards hospitals and specialized clinical environments, but also towards the patient's environments, such as the patient's house, senior citizen residence, or gym, and mobile environments such as an ambulance, mobile clinics, and travel health services, where support for mobility will be required.

In addition, IoT will offer higher integration, since it is focused on its integration and interoperability within the very current information infrastructure and e-Health platforms, instead of offering an additional alternative to the market. This integration factor is the key element, as stated by Dr Najeeb Al-Shorbaji, director of knowledge management and sharing at the World Health Organization (WHO), *"It cannot be viewed as a standalone proposition and must be seen as a subset of e-health, which in turn is an integral part of a more general, comprehensive healthcare strategy, encompassing all security, ethical and standards issues"* [13]. This integrator spirit is fundamental to the current Internet and IoT.

The applications of the IoT in clinical environments range from basic monitoring applications for eventual measure of the physiological status with devices such as glucometers, pulse oximeters and blood pressure, to wearable clinical devices for continuous monitoring of vital signs such as electrocardiograms, 24-hour ambulatory blood pressure and insulin pumps.

The use of the IoT for clinical devices enables remote monitoring of vital signs and patient status. In addition, this allows to link the data from the patient with external knowledge-based information systems to analyze the status, trigger alarms when anomalies are detected, and even remote support.

Several organizations and alliances working in the standardization of the IoT are considering the clinical environments as one of the main use cases. Specifically, the European Telecommunications Standards Institute (ETSI) Technical Committee (TC) M2M, the ETSI TC e-Health [14], the mentioned ITU-T, IEEE with the IEEE 1073 family of standards (elaborated in conjunction with the European Committee for Standardization (CEN) and the International Organization for Standardization (ISO) [15]), and finally industrial organizations such as Continua Alliance [16], ZigBee Alliance [17], and Internet Protocol for Smart Objects (IPSO) Alliance [18].

II. Key challenges

IoT and ubiquitous integration of clinical environments define complex design challenges and requirements in order to reach a suitable technology maturity for its wide deployment and market integration. From the beginning, IoT devices present inherited challenges since they are constrained devices with low memory, processing, communication and energy capabilities.

The first key challenge for a ubiquitous deployment is the integration of multi-technology networks in a common all-IP network to ensure that the communication network is reliable and scalable. For this purpose, IoT relies on the connectivity and reliability for its communications on Future Internet architecture and the IPv6 protocol to cover the addressing and scalability requirements.

The second key challenge is to guarantee security, privacy, integrity of information and user confidentiality. The majority of the IoT applications need to take into considerations the support of mechanisms to carry out the authentication, authorization, access control, and key management. In addition, due to the reduced capabilities from the constrained devices enabled with Internet connectivity, a higher protection of the edge networks needs to be considered with respect to the global network.

The third key challenge is to offer support for the mobility, since the Future Internet presents a more ubiquitous and mobile Internet. Mobility support increases the applicability of Internet to new areas. The most present nowadays are mobile platforms such as smart phones and tablets which enable a tremendous range of applications based on ubiquitous location, context awareness, social networking, and interaction with the environment. Future Internet potential is not limited to mobile platforms, else IoT is another emerging area of the Future Internet, which is offering a high integration of the cybernetic and physical world. Therefore, since the physical world is mobile and dynamic, IoT will require support mobile and dynamic ecosystems.

Mobility support in the IoT enables a global and continuous connection of all the devices without requiring the disruption of the communication sessions. For example, mobility management in hospitals is required since clinical devices can be connected through wireless technologies. Mobility offers highly valuable features such as higher quality of experiences for the patients, since this allows the patients to move freely, continuous monitoring through portable/wearable sensors, extend the coverage within all the hospital, and finally a higher fault tolerance since the mobility management allows the connection to adapt dynamically to different access points. Therefore, clinical environment is one of the main scenarios where the mobility for the IoT-based applications exploit these capabilities, in terms of fault tolerance influences directly in the life support, and continuous monitoring influences the quantity of data available which is required for real-time diagnostic.

Finally, other challenges are also arising from the application, economical, and technological perspectives. For example, from an application point of view are the requirements for processing large amounts of data for a growing number of devices, it is the so-called *Big Data*. From the economic points of view, the needs to provide economies of scale, i.e., new services based on existing modules in order to leverage the

related platform investment. From the networking point of view to offer an end-to-end support for Quality of Service (QoS), since the different IoT applications will present different requirements in terms of latency and bandwidth, for example, for clinical environments the traffic should be prioritized over other non-critical traffic coming from smart-metering.

The following subsections describe in more detail the current status of the challenges, and describe the goals considered for this thesis in order to contribute to the solution of them, in terms of heterogeneity, connectivity/reliability, security and mobility.

Heterogeneity

IoT started focusing on building blocks such as Radio Frequency IDentification (RFID), due to its capabilities of identifying the uniqueness of an object in the world. After that initial approach, the technology evolved and the IoT was not much more a metaphor for RFID capabilities, else it was feasible that the devices such as sensors and appliances were connected to the IoT. Thereby, it was giving birth to smart things and smart objects concepts, as an evolution of the devices located at the Wireless Sensor Networks (WSN) with IPv6 connectivity through protocols such as the mentioned 6LoWPAN [19].

IoT market is developing new technologies such as WiFi Low Power, Bluetooth Low Energy, IEEE 802.15.4g, and Near Field Communications (NFC), which are the evolution of the initial RFID and WSN (IEEE 802.15.4) towards very well-known and interoperable technologies with the new generation of personal devices such as laptops, tablets and smart phones.

IoT deployments are not limited to RFID, WSN and the mentioned emerging technologies; the majority of the IoT scenarios and ecosystems are composed of heterogeneous IoT devices based on different technologies with different capabilities such as legacy building automation technologies (e.g., BACnet, Konnex, X10), industrial devices based on industrial protocols (e.g., Control Area Network (CAN), M-BUS, Wireless M-BUS), smart grid technologies (e.g., smart metering), and smart cities technologies (e.g., parking pots, street lights, environmental sensors).

For example, deployments in clinical environments cover multiple types of devices ranging from passive things to active things. An IoT-based clinical environment can be composed of the wheelchairs, drugs and instruments that are tagged with RFID passive tags, and also of active things such as patient monitors, clinical devices, appliances, and personal devices (e.g., laptops, smart phones, tablets).

In conclusion, since IoT ecosystems will be composed of a high range of technologies, a suitable support for the heterogeneity needs to be provided by the IoT communication architecture. The goals are firstly, to evaluate the capabilities of 6LoWPAN based on IEEE 802.15.4 for IoT applications and clinical environments. Second, to evaluate the capabilities of the IoT for emerging technologies such as NFC as an evolution of RFID, and Bluetooth Low Energy as an evolution of initial WSNs, and finally, to develop a

communication architecture that allows the integration of heterogeneous devices in a common environment.

Connectivity and reliability

The number of devices that are connected to the Internet is growing exponentially. This has led to defining a new conception of Internet, the commonly called Future Internet, which started with a new version of the Internet Protocol (IPv6) that extends the addressing space in order to support all the emerging Internet-enabled devices.

IPv6 is the fundamental technology for the IoT. It is estimated that several billion things will be connected by 2020. Unlike IPv4, IPv6 can address this number of objects. The IPv6 address space supports 2^{128} unique addresses (approximately $3.4 * 10^{38}$). Specifically, it can offer $1.7 * 10^{17}$ addresses on an area about the size of the tip of a pen. The advantages of the IPv6 integration in the IoT are not limited to a universal addressing space; its main advantages are to offer stable, scalable, extensive, and tested protocols for global end-to-end communication, device/service discovery, mobility, end-to-end security, and other relevant features such as stateless addressing auto-configuration, multicast addressing for group operations, and its flexibility for the application layer with technologies such as Web Services.

IPv6 has been designed to provide secure communications to users and all the devices attached to the them; thereby users are always connected.

IPv6 features are what have made possible thinking about connecting all the objects and build the IoT. The objective of IoT is the integration and unification of all communications systems that surround us. Hence, the systems can get a control and access total to the other systems for leading to provide ubiquitous communication and computing with the purpose of defining a new generation of services.

IoT is enabled by tiny and highly constrained devices, so-called smart objects. These devices have low-performance properties due to their constraints in terms of memory capacity, computation capability and energy autonomy. In addition, their communication capabilities present a low bandwidth, limited reachability because of the usage of hard duty cycles and consequently unstable connectivity for solution with a very low duty cycle and high power constraint.

These devices with constrained connectivity and communication capacity are what we can find, from some years ago, in the Low-power Wireless Personal Area Networks (LoWPANs).

The IETF working group has defined IPv6 over that LoWPANs (6LoWPAN) to extend Internet to smart devices [20]. 6LoWPAN offers the LoWPANs all the advantages from IP such as scalability, flexibility, well tested, extended, ubiquitous, open, and end-to-end connectivity.

It could be considered that 6LoWPAN devices are also empowered with IP protocols, i.e., protocol for mobility such as MIPv6, management such as SNMP, security such as IPSec, etc. However it is not feasible for 6LoWPAN devices to be associated with host-based protocols such as mobility, management, security etc. because 6LoWPAN nodes are energy and resource constrained. Host-based protocols require most

of the signaling on end nodes and because the design features of 6LoWPAN network were not considered in the design issues of the host-based protocols. For example, a 6LoWPAN node may run out of energy causing a fault in the network. This has restrictions in size packets and presents aggressive techniques to conserve energy by using sleep schedules with long sleep periods, devices just wake up to receive IPv6 signaling messages. This feature introduces delays in the reception of messages because they are not attended to until the node wakes up. Therefore, these delays, power restrictions, packet size restrictions etc. are not considered in the current IPv6 protocols.

The goal to solve the initial challenge for connectivity and reliability is to move toward the common addressing space of Internet (IPv6) to all the resources and devices available in an IoT ecosystem. In this manner, an Internet of everything can be reached.

Security

Security is a wide concept which covers everything from authenticity (ensuring that the end-user is who is claimed to be), authority (ensuring that the end-user is allowed to perform the requested action), integrity (the data received is exactly the same data transmitted), and confidentiality (communication is not understandable for intermediary users, even when an intruder is in the network). These concepts are satisfied through a set of protocols, algorithms and cryptographic primitives.

The IoT security has been one of the most discussed and yet pending issues, even after of the existence of protocols for IPv6 network security such as IPSec, and for datagrams (i.e., UDP or CoAP) such as DTLS. Security for the IoT is not excessively extended and deployed because of the difficulties in configuring (IPSec) for end users and the lack of scalable certificate management for DTLS. Consequently, the majority of the Internet traffic continues being transmitted in plain text, i.e., unprotected.

For that reason, one of the initial actions in order to carry out an effective deployment of autonomous and unassisted IoT deployments that satisfies the scalability and self-management requirements from the IoT is the development of protocols for authentication and key management.

Specifically, on the one hand, the protocol for the authentication and key management at the network layer such as the Protocol for Carrying Authentication for Network Access (PANA) [21] is being considered by the research institutions and also industrial alliances, such as the ZigBee Alliance for their ZigBee IP stack [22].

On the other hand, the IPSec set of protocols (i.e., Internet Key Exchange (IKE) and Encapsulation Security Protocol (ESP)), and another protocols at the medium access layer such as 802.1x, are also being considered. All of these share the usage of the Extensible Authentication Protocol (EAP) to transport the security credentials.

Therefore, the challenge is not limited to the protocol, else the EAP scheme needs to be optimized in terms of a proper support of the required cryptographic primitives by the constrained device, i.e., symmetric cryptography algorithm to protect the packet, hash function to ensure the integrity and authenticate of the packet, and finally asymmetric cryptographic algorithm to carry out the key exchange and initial authentication.

Some initial works for the IoT have been proposed for IPSec [23], where several pending problems have been found, since for example a low version of the symmetric cryptography with 32-bit keys is used, such as AES-CBC-32, which are very weak. In addition, this relies on pre-shared keys for IPsec, which is not very scalable. Therefore, it does not solve the scalability and self-management requirements.

In order to satisfy these requirements, a Key Management Protocol (KMP) can be considered, that allows keys to be refreshed periodically (therefore maintaining acceptable security levels). Specifically, an automatic key exchange mechanism is required; thereby, each node can keep track of the security associations (SA) that specify how a particular IP flow should be treated in terms of security.

The most extended KMP is IKE. A very simple approach of IKE has been defined in [24], which does not satisfy all the requirements and functionality for a full SA establishment.

Other issues from IPSec is that the overhead caused by a IPsec packet (the extra bytes on the IP header) can force the packet to be fragmented (the link layer payload that includes the extra IPsec bytes becomes bigger than the maximum size of a 802.15.4 packet), thus an extra packet must be sent to the link layer and the energy/network overhead will become bigger. In addition, this overhead problem is worse with the ESP mode of IPSec, since the internal headers of IPv6 and UDP are encrypted and consequently cannot be compressed.

In addition to IPSec, the majority of works from the CORE Working Group in IETF are focused on the integration of security through the transport layer security solutions such as DTLS for CoAP. DTLS is the default security for CoAP.

A pre-shared key mode (PSK) is also considered by CoAP, with the aforementioned problems regarding the lack of scalability for this pre-establishment of the security credentials.

CoAP also offers a very interesting approach based on RawPublicKey, i.e., a solution based on the use of an asymmetric key pair, but without an X.509 certificate metadata. This approach is highly relevant since it can manage the identity issues mentioned in the introduction section, in order to verify the authenticity of the device and its link with the manufacturer. For example, the Certification Authority (CA) of the public key can also indicate the list of identities of the nodes, with which it can communicate. It can thereby indicate the entities which are trustworthy in the initial verification and bootstrapping phase.

CoAP also considers certificates, i.e., X.509 certificate that binds it to its Authority Name and is signed by some common trust root, e.g., the manufacturer.

In order to optimize DTLS for smart objects, DTLS 1.2 [25] offers the schemes to re-use the cryptographic hardware support by the majority of the IEEE 802.15.4 transceivers for the symmetric cryptography, i.e., AES CCM. In addition, considers the usage of Elliptic Curve Cryptography (ECC) for the asymmetric cryptography. Thereby, making it more suitable for these constrained devices.

Nowadays, DTLS is being considered by the Smart Energy profile for ZigBee alliance (SE 2.0), and it is also being considered as an adaptation of DTLS 1.2 in the IPSO Alliance based on the subset allowed by RFC6347.

In addition to the solutions presented, there is security support over the current Internet architecture based on IPv6 in the network layer and UDP/TCP for the transport layer, where the security is based on IPSec for IPv6 and DTLS/TLS for UDP/TCP respectively. Also two solutions from the IETF to support the ID/Locator split have been defined. The first, HIP, has been developed by the Host Identity Protocol (HIP) Working Group, a group mainly focused on improving security of the Future Internet, and the HIP Diet EXchange (HIP DEX) [26], which has been optimized for constrained environments such as the Internet of Things. HIP offers in a single mechanism the capabilities for authentication and establishment of the communication.

Therefore, the goals to solve for the security support are, first, to optimize cryptographic primitives for the described protocols. Specially, ECC for the asymmetric cryptography. Second, to analyze and evaluate the impact of IP security protocol (IPSec) for constrained devices. Finally, to analyze the possibilities for novel protocols that satisfies the scalability and self-management requirements.

Mobility

Mobility presents several challenges for the efficiency of networks and protocols, since mobility protocols have to deal with inherent characteristics of IoT such as hard duty cycles (i.e., long sleep period), reduced energy and processing capabilities, and constrained bandwidth.

Mobility management is composed of two fundamental phases, on the one hand, the movement detection in order to be aware of the device changing its location and consequently will require linking to an alternative network, on the other hand, the signaling and control messages required to be aware of changing locations, (i.e., network and locator), to the networks and clients relative to the device in movement.

Movement detection is solved through active scan, passive overhearing of messages from other protocols, or specific signaling from the mobility protocol.

Mobility signaling is being solved in different ways mainly split into two trends, on the one hand, a trend based on an evolutionary research following the IPv6-based approach and current Internet architecture, and on the other hand, a clean-slate, where new architectures are proposed that require major changes in the existing protocols and networking philosophy.

The clean-slate trend is based on new concepts such as ID/Locator split architectures such as those presented in LISP [27], developed by the Locator ID Separation Group (LISP) Working Group which is focused on improving the scalability of the routing for the Future Internet, and HIMALIS presented in [28].

HIMALIS architecture offers lightweight mobility management based on the ID/Locator split concept. The ID/Locator split architecture employs two different values, one for identification (*ID*) and another for location (*Locator*). Therefore, the device changes its Locator in the network layer when the device changes its position in the network topology. The most relevant aspect of this split is that the Locator changes

without requiring upper layers to change the ID, thereby ensuring that established communication sessions associated with the ID are not interrupted by mobility.

These kinds of architectures present the advantage that mobility is directly supported by the separation of the session identification with the locator of the device, which is the problem of the current Internet architecture. Previous works for the IoT have been focused on this approach, the main issue is that the overhead for 6LoWPAN devices is increased since there is the need to transport one additional header for the identification layer. These types of solutions are very relevant from the research point of view, but they present the main inconvenience of not being feasible, since the current hardware and infrastructure deployed is not ready for this kind of approach.

For that reason, the other trend is the evolutionary research approach; this follows the current Internet architecture for the management of the identification and location, i.e., IPv6 continues being used for *Identification* of the session in the transport and application layers, and *Locator* of the devices for routing in the network layer. These solutions allow continuing using the existing infrastructure and overcome the problem using a similar concept to the ID/Locator split but in an implicit way. Specifically, the main protocol following the evolutionary approach is Mobile IPv6 (MIPv6). MIPv6 uses two IPv6 addresses, fist, the initial address of the device, commonly denominated Home Address is used as identifier, and second, the new address in the visited network, commonly called care-of address, is used as locator.

MIPv6 protocol provides the signaling messages and IPv6 header extensions to manage the binding between these two addresses. In addition, this defines the security mechanisms and networking requirements in order to avoid the identity supplantation and man-in-the-middle attacks.

The main concerns of MIPv6 is that it presents a high overhead for the data packets when the mobile node is in roaming, since this needs to include the destination option to specify its Home Address in case of applied route optimization or build an IPv6 tunnel which requires an additional IPv6 header. Both cases require a high overhead.

The second problem with Mobile IPv6 is that IPSec is mandatory in order to protect the communications between the mobile node and the home agent. Such as mentioned, the trust relationship between the mobile node and the home agent is a fundamental requirement of MIPv6, since all the security of the binding update for the mapping between the care-of address and home address, and additional security processes such as the return routability for the route optimization are based on this trust relationship.

Therefore, the goals for the mobility support are, first, to design new techniques for fast movement detection. Second, to design and evaluate a lightweight implementation of MIPv6 to offer a secure and efficient mobility management for the IoT, and finally, to design and evaluate a solution based on ID/Locator split architecture that also ensures a secure and efficient mobility management.

III. Goals

The main goal is to address a communication architecture for the next generation of IoT applications, especially for clinical environments, that maximizes its efficiency and performance through high integration capabilities, seamless interaction between users and systems, and that provides suitable support for security and mobility.

The previous section has presented key challenges that need to be defined as goals in order to achieve an adequate communicate architecture with support to the homogeneous connectivity, reliability, security, mobility and the integration of the existing heterogeneity in technologies, devices and legacy protocols. Figure 1.1 summarizes the key requirements to be addressed by this thesis, in order to convert them into enablers that facilitate the development of the clinical environment market in areas such as diabetes, breathing problems, and drugs adherence.

This work has led to the offering of enablers to build a communication architecture that provides added value for the development of personalized healthcare services in ubiquitous clinical environments.

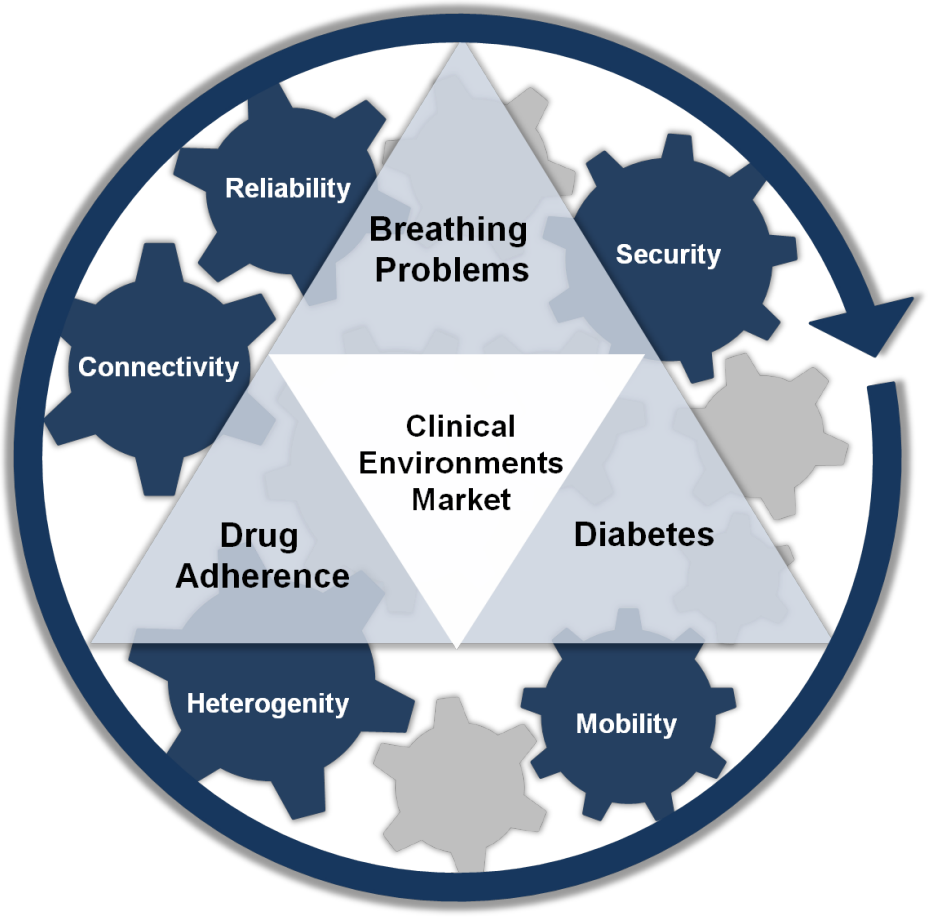


Figure 1.1: Key enablers addressed in this thesis to satisfy the requirements from the clinical environments market.

The goals considered for this thesis are presented in Figure 1.2, where the presented enablers are integrated to build the communication architecture that satisfies the described challenges to offer a communication architecture for clinical environments with scalable security and mobility.

The goals are defined as follows:

Heterogeneity

1. Design and development of a communication architecture that allows the integration of heterogeneous devices in a common environment.
2. Analyze and evaluate the capabilities of 6LoWPAN (IEEE 802.15.4), Near Field Communication (NFC) and Bluetooth Low Energy for IoT applications and above all for clinical environments.

Connectivity and reliability

3. Design IPv6 addressing mechanisms for emerging IoT technologies such as Bluetooth Low Energy and IEEE 802.15.4.
4. Design IPv6 addressing mechanisms for legacy technologies and devices in order to reach a common addressing space (IPv6) for all the resources in an IoT ecosystem.

Security

5. Optimize cryptographic primitives for constrained devices. Especially, Elliptic Curve Cryptography (ECC) for the asymmetric cryptography.
6. Design a novel protocol for authentication and secure communication establishment.
7. Analyze and evaluate the impact of IP security protocol (IPSec) for constrained devices.

Mobility

8. Design and evaluate a lightweight implementation of MIPv6 to offersecure and efficient mobility management.
9. Design and evaluate a solution based on ID/Locator split architecture that also ensures secure and efficient mobility management.

10. Design and evaluate novel techniques for movement detection in order to reach a fast and lightweight handover.

Clinical environments applications

11. Design a lightweight application protocol for clinical environments.

12. Evaluate the IoT capabilities for different clinical environments such as drugs adherence and breathing problems.

III.1. Communication architecture proposed to satisfy the goals

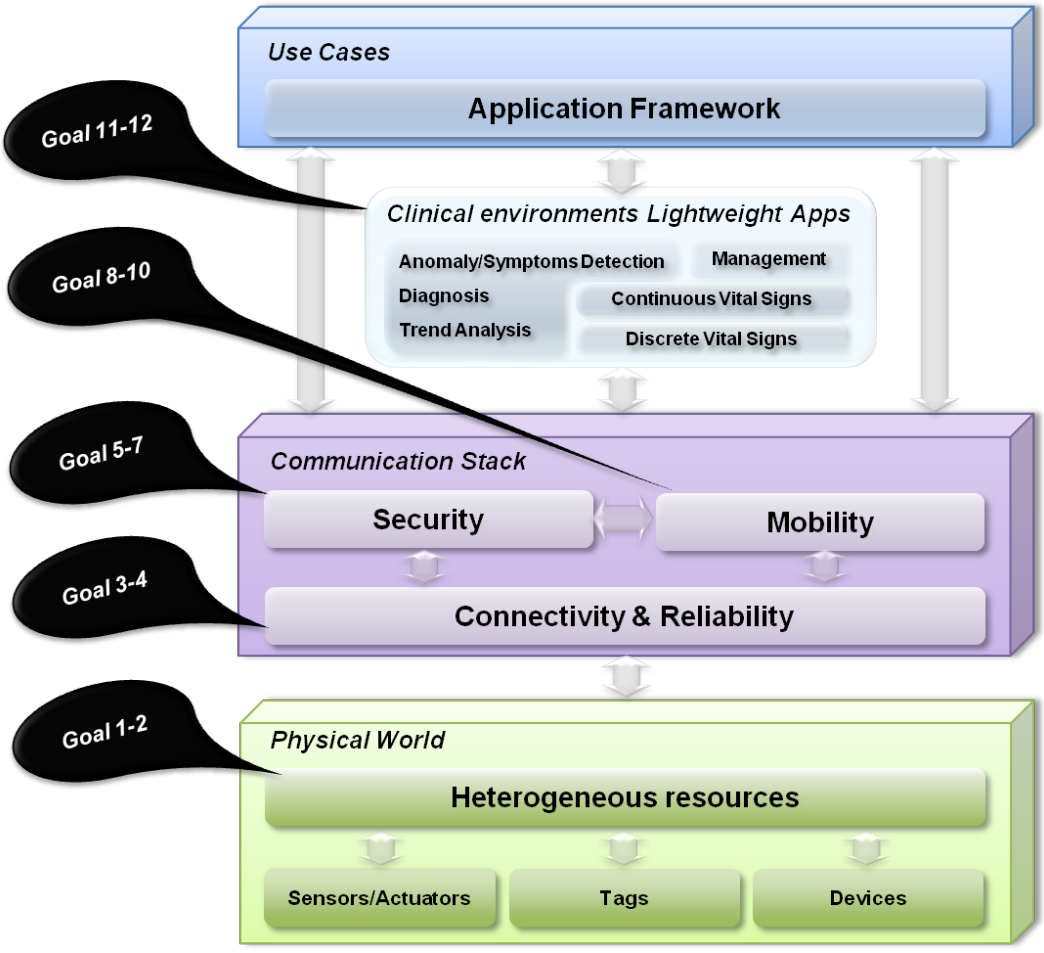


Figure 1.2: Goals to build and integrate the enablers into the proposed communication architecture.

Figure 1.2 presents the mapping of the goals with each one of the key components required to build a communication architecture for clinical environments based on the IoT to support scalable security and mobility.

The bottom level of the Figure 1.2 presents the integration of heterogeneous resources from the physical world. Specifically, this considers the support of active resources, e.g., devices, sensors and actuators from 6LoWPAN/IEEE 802.15.4 and Bluetooth Low Energy technologies, and also passive resources, e.g. tags and cards from RFID and NFC technologies.

The middle level of Figure 1.2 presents the communication stack to provide the protocols and mechanisms that make the interaction between the applications and the physical world feasible.

The communication stack grounds need to provide suitable connectivity and reliability for all the physical world devices based on Internet technology, i.e., IPv6.

Once connectivity and reliability is reached, then the communication stack needs to provide additional protocols and mechanisms built over IPv6 to offer suitable communication with support for security and seamless connectivity in the case of changes in the position or in the infrastructure, i.e., mobility.

The top level of Figure 1.2 presents the lightweight application protocol for clinical environments. This lightweight application protocol needs to be built on top of the communication stack in order to exploit the potential of the IoT and the IPv6-related protocols.

Finally, this application protocol needs to be evaluated in different clinical-based use cases with different requirements, i.e. from use cases with discrete vital sign monitoring, to use cases with the need for continuous monitoring.

III.2. Methodology

These goals have been satisfied and developed specifically with the following specific tasks:

- Analysis of the components required for the communications architecture in clinical environments. For this purpose, international experts such as Kaiser Permanente (USA), ELGA (Austria), Flowlab, and Mutua Terrasa (Spain) will be consulted.

- Design of a communications architecture and validation with the mentioned international experts.

- Analysis of the clinical devices required for the different use cases, technologies involved and their communication requirements.

- Evaluation of the suitability of 6LoWPAN, NFC and Bluetooth Low Energy to integrate the clinical devices and provide continuous monitoring.

- Design and development of a lightweight application protocol that makes the communication over the mentioned technologies for the requirements from the clinical devices feasible.
- Design mechanisms for IPv6 addressing everything. Specifically, on the one hand, a solution for programmable technologies such as Bluetooth Low Energy and 6LoWPAN, and on the other hand, for legacy technologies such as RFID, IrDA, Bluetooth Classic.
- Develop scalable support for the security of communications based on asymmetric cryptography, such as ECC, in order to offer autonomous distribution and commissioning, and scalable deployment and validation.
- Design a novel protocol for authentication and secure communication establishment based on ECC. Specifically, HIMALISEC for the secure authentication of nodes in the HIMALIS architecture has been defined.
- Evaluate the impact of IP security protocol (IPSec) for constrained devices and design and develop a lightweight version of IPSec in order to offer a solution based on IPv6.
- Design and evaluate a lightweight implementation of MIPv6 to offer secure and efficient mobility management.
- Design and evaluate a solution based on ID/Locator split architecture that also ensures secure and efficient mobility management.
- Design and evaluate novel techniques for movement detection in order to reach a fast and lightweight handover.
- Evaluate the IoT capabilities for different clinical environments such as cardiovascular diseases, drugs adherence, and breathing problems.

IV. Results

Figure 1.3 summarizes the key components that define the results of this thesis and the works presented in detail.

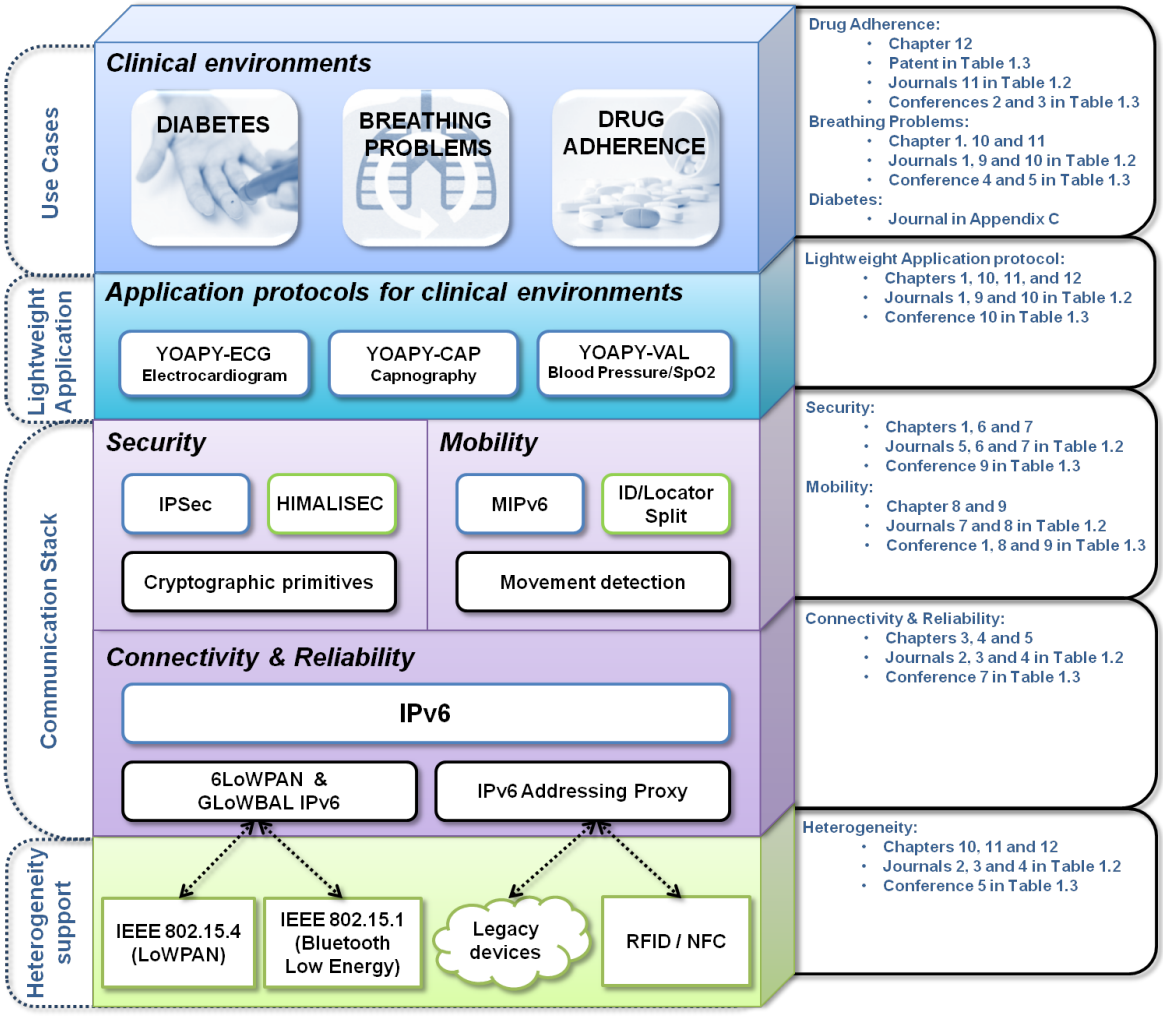


Figure 1.3: Communication Architecture for clinical environments based on the Internet of Things to support scalable security and mobility.

The first foundation of the proposed communication architecture has been the development of an interconnection framework to integrate the heterogeneous devices available in the IoT ecosystems.

Specifically, the devices supported by this interconnection framework consider technologies such as IEEE 802.15.4 (6LoWPAN), IEEE 802.15.1 (Bluetooth Low Energy), legacy devices and identification technologies such as RFID and NFC.

The interconnection framework for clinical environments is presented in Chapter 2. Chapter 2 identifies, communication requirements from the clinical environments, and the parties involved for the support of mobile health and remote monitoring.

This interconnection framework presents the limitations, requirements, and consequent challenges that will make the integration of IoT-based solutions into clinical environments feasible.

Specifically, these challenges are in terms of connectivity, reliability, security, mobility, and finally the optimization of the application protocols for integrating the heterogeneous devices found in the different use cases, and satisfying the trade-off between the quantity/quality of the data and the power consumption, i.e. autonomy of the devices.

IV.1. Connectivity and reliability

The bases of the interconnection framework are connectivity and reliability, from the networking point of view.

In order to satisfy these requirements, the interconnection framework has relied on Internet technology, in particular IPv6. Since, IPv6 is the main enabler for extending the Internet of Things to the Future Internet.

Chapter 3 presents how the architecture has been powered by the IPv6 connectivity in order to provide an homogeneous, scalable, and interoperable medium for integrating heterogeneous devices built on technologies such as 6LoWPAN, Bluetooth Low Energy, legacy devices and identification technologies.

In more detail, this thesis has proposed two novel solutions to enable ubiquitous connectivity and reliability, on the one hand, GLoWBAL IPv6 presented in the Chapter 4, and on the other the IPv6 Addressing Proxy for legacy technologies presented in the Chapter 5.

GLoWBAL IPv6 has been proposed to optimize global addressing involving smart devices such as that found in low power wireless personal area networks (LoWPAN) [29]. GLoWBAL IPv6 has the further advantage of providing efficient addressing and integration to both IEEE 802.15.4 sensor devices, which do not offer native support for 6LoWPAN, and also to other technologies which do not support IPv6 communication capability into their stacks.

GLoWBAL IPv6 defines an Access Address/Identifier (AAID) to reduce the overhead from the network and transport headers. AAID simplifies IPv6 and UDP communication parameters (source and destination addresses/ports, originally 36 bytes long) to a single 4-byte communication identifier augmented by one byte for the *Dispatch* header, totaling 5 bytes for the GLoWBAL IPv6 header. Thus, the IPv6/UDP headers are significantly reduced. This mechanism achieves an efficient frame format for global communications in networks that do not have native support for IPv6.

An example of its potential is described. Let take a heterogeneous device with a Bluetooth Low Energy interface, such as a smart phone with also Internet connectivity through the cellular network interface. GLoWBAL IPv6 fills the IPv6 addressing requirement for any smart thing connected to the smart phones through the Bluetooth Low Energy network by acting as the mapping protocol between the Local Network (capillary network) and the wide-area network (cellular network) using appropriately constructed IPv6 addresses. , Consequently this smart phone can efficiently enable with

IPv6 through GLoWBAL IPv6 to the smart things connected through its Bluetooth Low Energy interface. But, GLoWBAL IPv6 is not a suitable solution for all devices that need to be enabled IPv6, since all the devices do not offer programming capabilities such as a smart phone or a gateway. Examples of these devices can be found in the inherited legacy technologies from the industrial and building automation markets. These markets present a rather fragmented set of technologies. Each technology comes with a set of fit-for-purpose sensors and their respective application environments which lack efficient interoperability among them. Some associations of manufactures have been formed to build common technology frameworks, e.g., Konnex (KNX) for building automation. While such *de facto* standards present widespread adoption to date, this does not discourage use of other relevant protocols such as the emerging ZigBee and the older X10. Due to this fragmentation, the support of this heterogeneity in order to shift towards a common access and communication framework based on IPv6 is also considered.

For that reason, an additional solution has been proposed to embrace all existing native addressing schemes. This solution has defined IPv6 mappings for each native addressing scheme by use of an IPv6 Addressing Proxy which handles the translations between an IPv6 address and its corresponding technology addressing, i.e. the native addressing depends on the technology.

IPv6 Addressing Proxy provides a transparent mechanism for the users and devices to map the different addressing spaces from each legacy technology to a common IPv6 addressing space [30, 31]. Specifically, the IPv6 addressing proxy is a technology-dependent mechanism for mapping each device to the different sub-networks built under the IPv6 prefix addresses provided by the Internet Service Provider. The IPv6 addressing proxy enables IPv6 addressing to all the devices regardless of the device technology thus offering a scalable and homogeneous solution to interact with devices which do not support IPv6 addressing. The IPv6 addressing proxy has been implemented in a multi-protocol card, and its performance, scalability and interoperability through a protocol built over IPv6 has been evaluated successfully.

As a result Goal 1 *"design and development of a communication architecture that allows the integration of heterogeneous devices in a common environment"* is reached with the mentioned interconnection framework and is presented in Chapters 2 and 3. Additionally, Chapter 2 *"analyzes and evaluates the capabilities of 6LoWPAN (IEEE 802.15.4) for IoT applications and especially for clinical environments"*, thereby satisfying part of Goal 2.

GLoWBAL IPv6 protocol presented in Chapter 4 has *"designed an IPv6 addressing mechanisms for emerging IoT technologies such as Bluetooth Low Energy and IEEE 802.15.4"* satisfying Goal 3, and the IPv6 Addressing Proxy presented in Chapter 5 has *"designed IPv6 addressing mechanisms for legacy technologies and devices to reach a common addressing space (IPv6) for all the resources in an IoT ecosystem"* satisfying Goal 4.

IV.2. Scalable security and mobility

First the communication architecture supports connectivity and reliability with the heterogeneous resources thanks to the presented interconnection framework and the IPv6 features. Then, the communication architecture is required to offer higher communication capabilities such as security and mobility. For that reason, the next goal has been to support scalable security and mobility.

Security needs to be addressed from an independent point of view, since each technology offers a different security solution, or no-security. For that reason, the security has been analyzed over IPv6 with solutions such as IPSec, or over an Identification layer, which also allows abstraction of the under-layer protocols and technologies to a common identification space with solutions such as HIMALISEC.

But before describing these protocol approaches, security is founded in the cryptographic primitives, and consequently as a first step, the suitability of the symmetric and asymmetric cryptography for IoT-based devices and resources has been analyzed.

IV.2.1. Cryptographic primitives

With regards to the symmetric cryptography, it is supported by hardware in the majority of the transceivers used in the IoT such as the IEEE 802.15.4. Therefore, symmetric cryptography does not present major challenges, since the native support of the hardware for the AES-CBC and AES-CCM algorithms. The main inconvenience of symmetric cryptographic is the scalability, since it was not conceived for scenarios such as the IoT, in fact it was designed for deployments with additional mechanisms for the bootstrapping of the security credentials before starting the communication, or the usage of the Internet Key Exchange (IKE) protocol which in the end require the usage of asymmetric key cryptography to make them secure and scalable. Therefore, the main challenge is the support of the asymmetric cryptography in order to reach scalable security. The first result in this line has been the *"optimization of the cryptographic primitives for constrained devices. Specially, Elliptic Curve Cryptography (ECC) for the asymmetric cryptography"*. This work has a high mathematical foundation, which has been carried out in collaboration with Prof. Leandro Marin, expert in cryptography and applied mathematics. Asymmetric cryptography is applied to the different methods and mechanisms developed by the community such as the mentioned IPSec IKE. Asymmetric cryptography has been considered mandatory in order to satisfy scalability of security and the goal to build highly scalable and autonomous solutions. Specifically, Chapter 6 presents an optimization of the cryptographic primitives for constrained devices such as the 16-bits microprocessor MSP430 from Texas Instrument (commonly used in IoT devices such as 6LoWPAN, active RFID and DASH7), thereby satisfying Goal 5. In detail, the work presented in Chapter 6 solves the mathematical optimization of cryptographic primitives for asymmetric cryptography based on a special pseudo-Mersenne primes, which we have denominated *Shifting Primes*. These primes can be used for ECC primitives with 160-bit keys in a highly optimal way. Specifically, this allows us to carry out ECC scalar multiplication

within 5.42 million clock cycles over MSP430 devices without a hardware multiplier. This result reduces, for a microprocessor working at 8Mhz, the time required for the basic ECC protocols to the boundary of 1s (the key generation and the Diffie-Hellman protocol is basically only one scalar multiplication). This is even less time than offered by the TinyECC implementation for devices with fast multiplication hardware instruction [32].

In addition to these constrained devices, the usage of the *Shifting Primes* has also been considered for the 32-bits microprocessor JN5139 from NXP/Jennic based on OpenRISC architecture. This microprocessor presents higher capabilities and consequently offers higher performance for this operation. The initial version used for the interconnection framework presented in Chapter 2 presented a performance of 765ms. The current works of *Shifting Primes* for OpenRISC are reaching results of under 500ms [33].

Further to the cryptographic primitives, the security is used as part of the communications protocols that compose the communication architecture in order to support the authentication, key management and secure communication establishment. The security solutions proposed have been developed with mobility in mind, in order to ensure a suitable solution that satisfies both scalable security and mobility.

IV.2.2. ID/Locator split approach: HIMALIS and HIMALISEC

The first approach to support security and mobility is based on the clean-slate approach. This proposes new architectures that require major changes in the existing protocols and networking philosophy. The new architecture considered has been the Heterogeneity Inclusion and Mobility Adaptation through Locator and ID Separation (HIMALIS) architecture [28]. For HIMALIS a scalable mobility management scheme has been designed and developed that considers the requirements and constraints from the IoT, solving the possible security and privacy vulnerabilities of the original HIMALIS architecture. The proposed scheme is based on Return Routability and ECC-based asymmetric cryptography, in order to support scalable inter-domain authentication and secure location update and binding transfer for the mobility process.

Chapter 7 presents HIMALISEC, *"the designed protocol for authentication and secure communication establishment"*. HIMALISEC protocol has been developed over the novel HIMALIS architecture, satisfying Goal 6 from the security point of view.

HIMALISEC also *"designs and evaluates a solution based on ID/Locator split architecture that ensures a secure and efficient mobility management"*, satisfying also Goal 9.

ID/Locator split-based architecture presents the advantage of native mobility support by the separation of the session identification (ID) with the locator of the device, which is the problem with the current Internet architecture. Previous work for IoT has focused on this approach such as Host Identity Protocol (HIP) [26,34], the main issue is that the overhead for 6LoWPAN devices is increased since there is a need to transport one additional header from the identification layer. These types of solutions are very relevant from the research point of view, but their main inconvenience is that

they are not feasible in the short term, since the current hardware and infrastructure deployed is not ready for this kind of approach. For that reason, this thesis has also considered the evolutionary research approach built on top of IPv6.

IV.2.3. IPv6 approach: MIPV6 and IPSec

The other approach is evolutionary research following the IPv6-based approach and current Internet architecture.

The main protocol following the evolutionary approach, to support the mobility, is Mobile IPv6 (MIPv6). MIPv6 uses two IPv6 addresses, the initial address of the device, denominated Home Address, as identifier (ID), and the new address in the visited network, denominated care-of address, as Locator.

MIPv6 protocol provides the signaling messages and IPv6 header extensions to manage the binding between these two addresses. In addition, this defines the security mechanisms and networking requirements in order to avoid the identity replacement and man-in-the-middle attacks.

The feasibility of MIPv6 for constrained devices such as that considered for the IoT was initially analyzed in the work presented in [35]. These works concluded that MIPv6 presents a high overhead for the data packets when the mobile node is in roaming, since this needs to include the destination option to specify its home address in case of route optimization applied or build an IPv6 tunnel which requires an additional IPv6 header. For that reason, *" a lightweight implementation of MIPv6 to offer a secure and efficient mobility management has been designed and evaluated "*. Chapter 8 presents the lightweight design and implementation of MIPv6 that consequently satisfies Goal 8.

In addition, IPSec is analyzed in Chapter 8, as IPSec is mandatory for MIPv6 in order to ensure the trust relationship between the mobile node and the home agent. This communication protection between the mobile node and the home agent is a fundamental requirement of MIPv6, since all the security of the binding update for the mapping between the care-of address and home address, and additional security processes such as the return routability for the route optimization are based on this trust relationship. Therefore, *" the impact of IP security protocol (IPSec) for constrained devices is also analyzed and evaluated "*, covering Goal 7.

IPSec presents the difficulty that encapsulates an IPv6 packet inside another. The problem with this encapsulation is that the inner header cannot be compressed and optimized. Therefore, the overhead coming from the inner header (40 bytes) cannot be waived. For that reason, Chapter 8, analyzes the impact of MIPv6 with IPSec over 6LoWPAN networks and the conclusion is that the unique way to offer an interoperable integration of the mobility with MIPv6 is without route optimization and using IPSec only for tunneling/encapsulation. Consequently the inner header can also be compressed. However, this approach presents security vulnerabilities in the case that the application layer is not secure. For that reason, this work also analyzes the suitability of IPSec ESP to provide security to the encapsulated packet in order to avoid any security vulnerabilities.

IV.2.4. Ad-hoc solutions for clinical environments

In order to offer an integral and optimal solution to support security and mobility, ad-hoc solutions need to be defined. Ad-hoc solutions allow the mobility to be optimized in terms of power consumption, handover delay, and overhead. For example, an ad-hoc solution has been developed for critical environments that offers movement direction detection [36]. Specifically, *"a novel technique for movement detection has been designed and evaluated in order to reach a fast and lightweight handover"*, satisfying Goal 10.

This ad-hoc solution offers good performance, fast handover and an integral solution for security and mobility being aware of the IoT devices constraint, the unique concern is that it is not interoperable with MIPv6. Therefore, the requirements from the specific use case need to be analyzed. For example, when considering the requirements of hospital networks and patient monitoring. [37, 38], it has been verified that ad-hoc solutions offer adequate performance, and since interoperability is limited to the hospital domain, this is does not present any interoperability requirement with third party networks. However, for emerging scenarios such as smart cities, interoperability with deployed and existing infrastructure is a major requirement.

Ultimately, even when ad-hoc solutions can be defined to offer the optimized solutions for a specific scenario, the IPv6-based approach offers a suitable performance with homogeneous solution for a wide range of scenarios. For that reason, this thesis has considered IPv6 technologies as the main driver for the definition of solutions and applications based on the IoT.

IV.3. Application protocol

During the last few years the promoters of the IoT, from academia and industry, have been focused on empowering these constrained devices with the protocols and functions of Internet-enabled devices.

The initial steps, the constrained capabilities of the IoT devices and differences between IPv6 design issues, have led to develop lightweight versions of the existing protocols. These lightweight versions have the advantage that they continue being interoperable/translatable to the full implementations. For example, a lightweight implementation of the IP stack such as uIP [39] and header compression through the 6LoWPAN protocol [40] have been developed in order to reach Internet connectivity. In addition, as a generic and wide supported application protocol, Web Services through RESTFul architecture have also been adapted for the IoT devices with lightweight and compressed protocols such as the Constrained Application Protocol (CoAP) [5, 41]. CoAP is an equivalent to HTTP but considers the constraint issues of the IoT devices, with the capability to be mapped to HTTP and offer at least an equivalent potential, for some scenarios it is even able to offer higher capabilities, since it has been designed with the IoT-related scenarios and requirements in mind.

IPv6 and WebServices offer the primitives to build application protocols for different use cases, as the final purpose of the communication architecture is its usage and

exploitation for different applications and use cases. However, this requires definition on top of CoAP/IPv6 a description of the resources from the different application and used cases. For this purpose, application profiles and guidelines such as the Open Mobile Alliance Lightweight Device Management for M2M (OMA LWM2M) [42] and IPSO Application Guidelines [43] are being defined.

This thesis has focused on clinical environment use cases. Specifically, Chapter 2 presents the *"design of a lightweight application protocol for clinical environments"*, this communication protocol for clinical environments is denominated YOAPY, thereby satisfying Goal 11.

The YOAPY pre-processing and data aggregation module is based on domain knowledge in order to reduce overload and optimize payload size. YOAPY can be used on top of CoAP or inside of an OMA Web Object; in short what YOAPY provides is the content that is required to be exchanged for the different clinical devices considered in a clinical environment.

For this purpose, YOAPY carries out pre-processing to analyze the relevant parts from the vital sign to compress the gathered RAW data, and makes its continuous and real-time transmission feasible; YOAPY also presents a set of optimizations regarding power consumption through data aggregation, and introduces security, integrity, and privacy capabilities to communication.

YOAPY includes a diagnostic estimation based on the knowledge domain. For example, the electrocardiogram analysis is presented in [44]. This offers an analysis for illness such as ventricular hypertrophy and necrosis when the QRS interval is over 0,12 seconds, or hyperkalemia, hyperkalemia, early repolarization, and digoxin, when the interval QT is under 0,34 seconds, and others related with the polarity, e.g. if the polarity from U is different to the polarity from T, it signifies ischemic heart disease or hypokalemia.

The main description features for the capnography wave form are slope of phase and alpha angle. They allow determination of the status of the treatment. In addition, the etCO2 value determines, with low level, anomalies such as a diminution of the CO2, hypothermia, reduction of cardiac activity, an excess of alveolar ventilation, or hyperventilation, with a high level determinates excessive production of CO2, hyperthermia, sepsis, a decrease in alveolar ventilation, hyperventilation, or malfunction of the ventilator or a combination thereof.

YOAPY has been compared with respect to the standard for communication with clinical devices defined in the IEEE 1073 [15]. This standard is followed up by several products developed in the framework of the Continua Alliance [16, 45].

The main advantages of YOAPY is that this offers the possibility of carrying out continuous monitoring for medical devices such as an electrocardiogram, which is required for the monitoring of diseases such as breathing problems and cardiology. YOAPY integrates sensors such as the capnographer, which are not supported by any of the vendors and manufactures associated with the Continua Alliance. Third, the transmission overload from YOAPY is independent of the electrocardiogram sampling frequency; therefore YOAPY is calculated with high, accurate data provided by the clinical device. In addition, YOAPY values provide a way to identify anomalies, since

a domain-based pre-processing of the wave is carried out. Finally, YOAPY requires less data to be transmitted, thereby optimizing the battery lifetime. Finally, this small piece of information provides more information requiring less space for information systems.

IV.4. Use cases and communication architecture instances

The proposed communication architecture and YOAPY have been *evaluated for different clinical environments such as drugs adherence and breathing problems* and evaluated over different communications technologies such as 6LoWPAN (IEEE 802.15.4), Near Field Communication (NFC) and Bluetooth Low Energy. As a result satisfying Goal 11, and covering all the technologies considered in Goal 2 to evaluate the IoT capabilities in clinical environments.

Chapter 10 presents the evaluation of YOAPY over Bluetooth Low Energy for continuous monitoring of patients with cardiovascular diseases. Bluetooth Low Energy presents several advantages in terms of low power communications for discrete values. This is not compatible with Bluetooth Classic, but Bluetooth Low Energy is being integrated in the current generation of smart phones and laptops which makes it very relevant for its integration with existing personal devices. YOAPY has allowed the communication of clinical devices with personal devices over Bluetooth Low Energy, even when it has not been designed for continuous communications.

Chapter 11 presents the evaluation of YOAPY over Near Field Communication (NFC) for the interaction and continuous monitoring of patients with breathing problems. NFC is a very interesting technology for elderly people, since this allows a very simple interaction through the contact-less communication. For example, this permits reading of a glucometer value just by proximity of the smart phone to the glucometer.

The interaction between the patients and the clinical devices, based on the NFC technology, has been evaluated with a group of elderly people. This has demonstrated the potential of this technology which is promising for the coming years with respect to the beginning of mobile Health, where the pairing and establishment of communication through technologies such as Bluetooth Classic was presenting some barriers in terms of acceptance by end-users.

For the integration of the clinical devices with wireless communications (i.e., 6LoWPAN) and NFC, a novel IoT device for clinical purpose, called Movital, has been developed. Movital means *Mobile Vital Signs Monitoring*. Figure 1.4 presents the Movital board.

Movital adapts basic communication technologies such as USB/RS232/IrDA (A) to 6LoWPAN, to allow interaction of the collected data with other entities of the architecture. Movital also integrates NFC technology to allow the identification of patients in order to personalize services, and identification of the physician in terms of responsibility issues. There is a requirement in environments with multiple patients, such as a senior residence, to link patient data to physician identity.

Movital is the combination of the aforementioned new generation technologies, including SkyeModule M2, from SkyeTek (B) for contactless identification (RFID and NFC), and module NXP/Jennic JN5139 for 6LoWPAN (C). Finally, the switch (D) allows selection of the functionality mode.

The size of Movital has been minimized to credit card size for easier integration. Furthermore, it is powered with reachable lithium batteries to optimize lifetime. This leads to a compact module which acts as an efficient information exchange gateway between clinicians, patients and information infrastructure.

In addition to the described hardware components, the proposed communication architecture has been instanced in Movital.

Specifically, this integrates the asymmetric-key encryption based on ECC for YOAPY, which has been optimized for the JN5139 transceiver in order to support low cost, high performance, and secure authentication, i.e. this integrates the asymmetric-key encryption presented in Chapter 6 over YOAPY, the integration with YOAPY is presented in the 2.

Movital also offers support for mobility and security based on IPv6, with the support of the lightweight versions of MIPv6 and IPSec presented in the Chapter 8.

Movital has been integrated with the patient's monitors such as presented in the Figure 1.5, with glucometers such as described in the Appendix B [10], and also other sensors such as Peak Flow Meters, electrocardiograms, blood pressure, and the pulse oximeter for the different use cases described in this work.

Figure 1.5 presents the integration as a piggyback box (A) for the 6LoWPAN transceiver (B) and RFID/NFC reader (C). Figure 1.7 presents how the different modules presented in this thesis for the communication architecture are instanced in Movital. In addition, this diagram presents the other information systems and platforms available in the interconnection framework. For example, a gateway called MONERE to connect Movital to the broadband Internet has also been developed, and third party information systems can be integrated such as the Hospital Information System (HIS) from the Hospital with the support of the Personal Health Record (PHR) to integrate the data from remote and mobile monitoring, the Service Provider System (SPS) to offer specific services of tele-health, and finally the Knowledge-Based Systems to support the diagnosis and analysis of the patient's status and behavior. An instance of these Knowledge-Based Systems has been developed for the detection of adverse drugs reactions in the drugs adherence use case.

The Chapter 12 presents the evaluation of RFID/NFC for drugs adherence and adverse drugs reactions. This usages RFID/NFC tags for the identification of drugs, in order to identify each drug dispenser when the dosage needs to be consumed. In addition to this solution based on RFID/NFC, an additional solution based on IrDA has been developed in collaboration with the World Health Organization (WHO) [46] in order to offer a low cost solution. Finally, it has been also patented an IoT device denominated HIGEA for drug adherence [47], which is presented in the Figure 1.6. HIGEA offers a smart blister to detect how many pills are being consumed and are left on the blister. This offers an application to follows-up the adherence, and finally

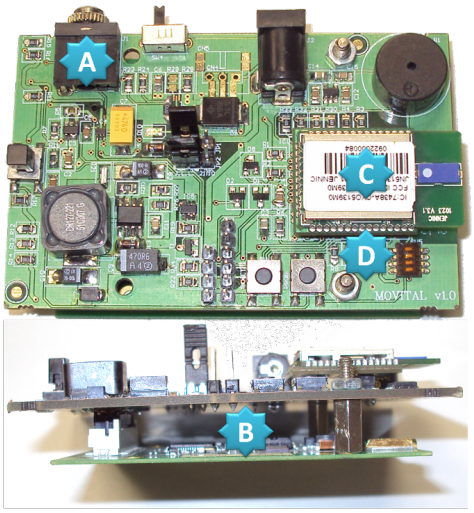


Figure 1.4: Movital device to adapt the off-the-shell devices and protocols to the IoT.

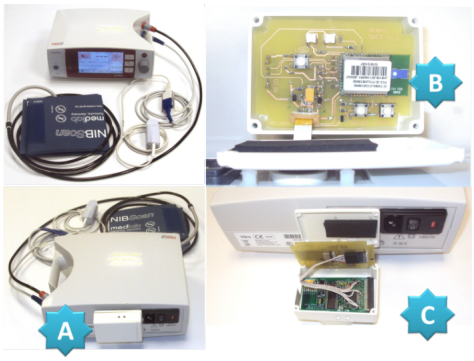


Figure 1.5: Patient monitor with an adapted version of Movital integrated.

Figure 1.6: Smart blister for drug adherence based on IoT technologies.

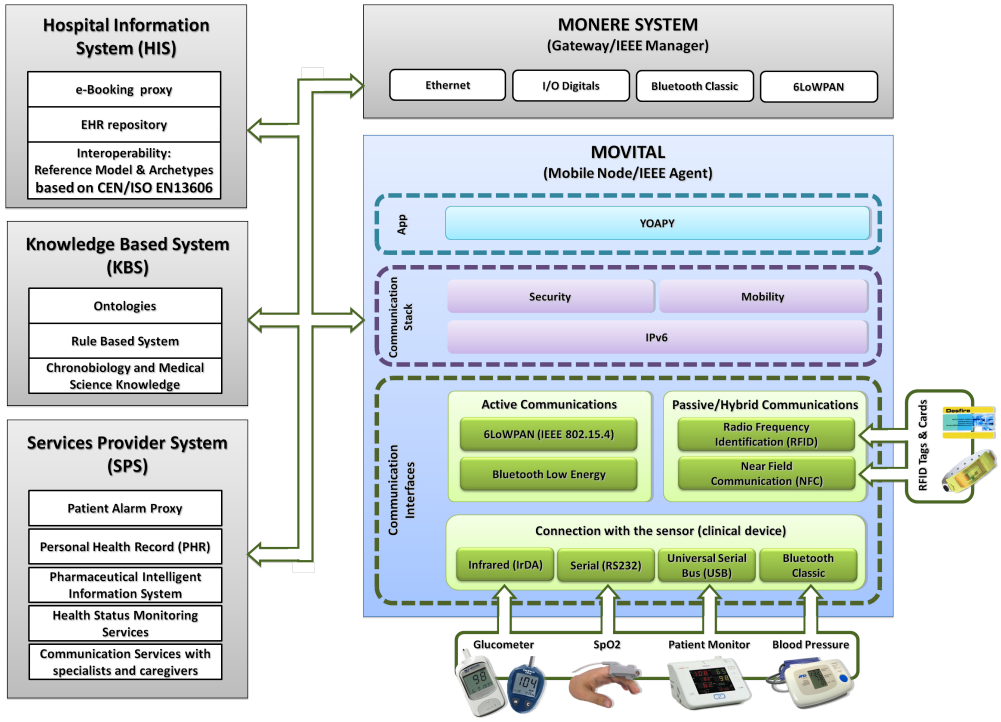


Figure 1.7: Integration of the proposed communication architecture in Movital for the different use cases.

this integrated Bluetooth Classic communication for its interoperability with personal devices.

The presented solution satisfies a bottom-up approach from the sensors where the data is collected to the clinical environments applications, satisfying all the mentioned challenges and goals in terms of heterogeneity, connectivity, reliability, security, mobility, and lightweight applications.

IV.5. Summary of the results

The following tables describe the main journals and conferences where have been presented the works that compose this thesis. On the one hand, the Table 1.1 presents the journal papers that compose this compendium. On the other hand, the Table 1.2 presents the Top 10 contributions to conferences of the initial approaches of the results finally published in the journals, and the patent with the drugs dispenser (HIGEA).

Table 1.1: Journal papers that compose this compendium.

No.	Description	Impact Factor
1	A. J. Jara, M. A. Zamora, and A. F. Skarmeta: Interconnection framework for mHealth and remote monitoring based on the Internet of Things, IEEE Journal on Selected Areas in Communications (J-SAC), DOI: 10.1109/JSAC.2013.SUP.0513005 2013, Vol. 31, No. 9, pp. 47-65	3,413 (2011)
2	Antonio J. Jara, S. Varakliotis, A. F. Skarmeta, and P. Kirstein: Extending the Internet of Things to the Future Internet through IPv6 support, Mobile Information Systems, IOS Press, DOI: 10.3233/MIS-130169, Vol. 9, 2013	2,432 (2011)
3	Antonio J. Jara, M. A. Zamora, and A. F. Skarmeta: GLoWBAL IP: An adaptive and transparent IPv6 integration in the Internet of Things, Mobile Information Systems, IOS Press, DOI: 10.3233/MIS-2012-0138, Vol. 8, No. 3, pp. 177-197, 2012	2,432 (2011)
4	Antonio J. Jara, P. Moreno-Sanchez, A. F. Skarmeta, S. Varakliotis, and P. Kirstein: IPv6 addressing Proxy: Mapping native addressing from legacy technologies and devices to the IoT (IPv6), Sensors, MDPI, DOI: 10.3390/s130506687, Vol. 13, No. 5, pp. 6687-6712, 2013	1,739 (2011)
5	L. Marin, Antonio J. Jara, and A. F. Skarmeta: Shifting primes: Optimizing ECC for 16-bit devices without hardware multiplier, Math. and Computer Modelling, ELSEVIER, DOI: 10.1016/j.mcm.2013.02.008, Vol. 57, No. 5, pp. 1155–1174, 2013	1,346 (2011))
6	Antonio J. Jara, Ved P. Kafle, and Antonio F. Skarmeta: Secure and Scalable Mobility Management Scheme for the IoT Integration in the Future Internet Architecture, Int. Journal of Ad-Hoc and Ubiquitous Computing, Inderscience, DOI: 10.1504/IJAHUC.2013.055468, Vol. 13, No. 3-4, pp. 228-242, 2013	0,848 (2011)
7	Antonio J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta: Lightweight MIPv6 with IPSec support: A mobility protocol for enabling transparent IPv6 mobility in the IoT with support to the security, Mobile Information Systems, IOS Press, DOI: 10.3233/MIS-2012-0138, Vol. 9, 2013	2,432 (2011)
8	Antonio J. Jara, R. M. Silva, J. S. Silva, M. A. Zamora, and A. F. Skarmeta: Mobile IP-Based Protocol for WPANs in Critical Environments, Wireless Personal Communications, Springer, DOI: 10.1007/s11277-011-0428-y, Vol. 61, No. 4, pp. 711-737, 2011	0,458 (2011)
9	Antonio J. Jara, P. Lopez, D. Fernandez, M. A. Zamora, A. F. Skarmeta, and L. Marin: Evaluation of Bluetooth Low Energy capabilities for tele-mobile monitoring in home-care, Journal of Universal Computer Science, Graz University of Technology, Vol. 19, No. 9, pp. 1219-1241, 2013	0,669 (2011)
10	Antonio J. Jara, P. Lopez, D. Fernandez, M. A. Zamora, B. Ubeda, and A. F. Skarmeta: Communication protocol for enabling continuous monitoring of elderly people through Near Field Communications, Interacting with Computers, Oxford Journals, DOI: 10.1093/iwc/iwt030, Vol. 25, 2013	1,233 (2011)
11	A. J. Jara, M. A. Zamora, and A. F. Skarmeta: Drug identification and interaction checker based on IoT to minimize adverse drug reactions and improve drug compliance, Personal and Ubiquitous Computing, Springer-Verlag, DOI: 10.1007/s00779-012-0622-2, Vol. 15, No. 4, pp. 431-440, 2012	0,938 (2011)

Table 1.2: Top 10 conference contributions and patent.

No.	Description	Impact Factor
1	Antonio J. Jara, Ricardo M. Silva, Jorge S. Silva, Miguel A. Zamora, and Antonio F. Skarmeta: Mobile IPv6 over Wireless Sensor Networks (6LoWPAN) Issues and feasibility, 7th European Wireless Sensor Networks Conference, EWSN 2010, ISBN: 978-989-96001-3-3. pp: 65-69. 2010.	CORE A
2	Antonio J. Jara, Francisco Belchi, Alberto Alcolea, Jose Santa, Miguel A. Zamora, and Antonio F. Skarmeta: A Pharmaceutical Intelligent Information System to Detect Allergies and Adverse Drugs Reactions based on IoT, 8th IEEE International Conference on Pervasive Computing and Communications (PerCom), ISBN: 978-1-4244-5328-3, 2010.	CORE A+ Oracle/Sun Microsystems Award to the best idea of the Web of Things
3	Antonio J. Jara, Alberto Alcolea, Mona Alsaedy, Miguel A. Zamora, and Antonio F. Skarmeta: Drugs Interaction checker based on IoT, IEEE Internet of Things conference, ISBN: 978-1-4244-7414-1, 2010	Top IoT Conference
4	Antonio J. Jara, David Fernandez, Pablo Lopez, Miguel A. Zamora, Benito Ubeda, and Antonio F. Skarmeta: Heart monitoring system based on NFC for continuous analysis and preprocessing of wireless vital signs, IEEE EMBS 5th International Conference on Health Informatics, ISBN: 978-989-8425-93-5, 2012	Top Health Informatics Conference
5	Antonio J. Jara, Pablo Lopez, David Fernandez, Miguel A. Zamora, Benito Ubeda, and Antonio F. Skarmeta: Interaction of patients with breathing problems through NFC in Ambient Assisted Living environments, IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, ISBN: 978-1-4673-1328-5, 2012	Best Paper Award
6	Miguel Castro, Antonio J. Jara, and Antonio F. Skarmeta: Smart Lighting solutions for Smart Cities, The 27th IEEE International Conference on. Advanced Information Networking and Applications (AINA-2013), 2013	Best Paper Award
7	Antonio J. Jara, Pedro Moreno, Antonio F. Skarmeta, Socrates Varakliotisy, and Peter Kirstein: IPv6 addressing proxy: Mapping native addressing from legacy communication technologies and protocols to IPv6 and the Internet of Things, IEEE International Conference on the Internet of Things (IoT 2012), 2012	Top IoT Conference
8	Antonio J. Jara, Miguel A. Zamora, and Antonio F. Skarmeta: Intra-mobility for Hospital Wireless Sensor Networks based on 6LoWPAN, 6th International Conference on Wireless and Mobile Communications, IEEE, ISBN: 978-0-7695-4182-2/10, 2010	
9	Antonio J. Jara, Miguel A. Zamora, and Antonio F. Skarmeta: An architecture based on Internet of Things to support mobility and security in medical environments, 7th Annual IEEE Consumer Communications and Networking Conference (CCNC), ISBN: 978-0-7695-4182-2/10, 2010	
10	Robert S. H. Istepanian, Antonio J. Jara, Nada Philip, and Ala Sungoor: Internet of Things for m-Health applications (IoMT), AMA-IEEE EMBS Medical Technology Conference, 2010	
11	Antonio F. Skarmeta, Miguel A. Zamora, Antonio J. Jara, Jose Lopez, Alfredo Quesada: System, device and method for detection of encapsulated objects. Application no: P-201230267-SE, 2012)	Being exploited by: Flowlab S.L. (See Figure 1.6)

V. Conclusions

This thesis has presented a communication architecture for clinical environments based on the Internet of Things (IoT) to support scalable security and mobility.

IoT defines the basis to reach a ubiquitous and mobile integration of the clinical environments with support for large scale connectivity from different physiological sensors, integration with information systems, and its homogeneous access through Internet and Web technologies from consumer devices such as tablets, smart phones, and laptops.

This thesis presents the contributions carried out to move from a conceptual IoT to a real one, where its potential has been developed, evolved, and demonstrated with the development of a set of modules based on the evolution of existing technologies and also in the design and development of new ones.

Consequently, this thesis has transformed the initial potential in useful capabilities to improve accessibility to clinical services, compatibility and ubiquity, enhancing citizen mobility, and guarantees access to medical information, anywhere and anytime.

For this purpose, this thesis has defined an interconnection framework which goes from the clinical devices integration, based on several technologies to the application protocol for clinical environments to interoperate and interconnect the clinical devices with the different applications and information systems available in a clinical ecosystem. The integration of the application protocol with the clinical devices is supported by the designed and developed full communication architecture; the communication architecture is composed of the key components to enable security, mobility, and end-to-end connectivity/reliability.

For the integration of the different clinical devices, this thesis has evaluated the capabilities of the IoT technologies, i.e., 6LoWPAN (IEEE 802.15.4), Bluetooth Low Energy (IEEE 802.15.1) and Near Field Communication (NFC) to support continuous monitoring of vital signs through physiological sensors.

The constrained capabilities of these technologies have presented excessive impact in terms of communication requirements, delay, and power consumption for the continuous vital signs, making the direct integration of the original signal from the physiological sensors using these technologies, unfeasible. For that reason, this thesis has presented a novel pre-processing and aggregation protocol, called YOAPY. YOAPY satisfies the communication requirements in aspects such as scalability, robustness, security, and privacy. This has been optimized to present a low overload, optimize the lifetime of the clinical devices, and provide a set of relevant data to the nurses and caregivers in aspects such as possible anomalies and the status of the patient. This is not only limited to the transmission performance in bandwidth, overload, and power consumption, it has also addressed high level requirements such as Quality of Service and Quality of Privacy. For that reason, performance based on latency, and security has been evaluated. The evaluation has been carried out over several days, and an intensive long time test of 24 hours to evaluate the total amount of data required per day, and the integrity together with the stability of the communications has been carried out.

YOAPY is supported by the developed communication architecture to offer also the key components for enabling connectivity, reliability, support for the heterogeneity, security and mobility.

Specifically, the first key contribution of this communication architecture has been the proposal of a set of technologies, i.e., GLoWBAL IPv6 and the IPv6 Addressing Proxy, for the inclusion of all the resources and devices available in the IoT ecosystem to the common addressing space from Internet (IPv6). As a result, an Internet of everything can be reached.

The proposed communication architecture has been designed to offer proper support of scalable security and mobility.

For this purpose, two different approaches have been addressed, on the one hand, a clean-slate approach, and on the other hand, an evolutionary approach.

For the clean-slate approach, a new architecture for Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation (HIMALIS) is considered. This architecture supports mobility through the ID/Locator split principle, and security through the designed HIMALISEC protocol. This approach requires major changes in the existing protocols and networking philosophy, for that reason, even when this offers a proper support for security and mobility, the evolutionary approach has been considered.

The evolutionary research approach follows the IPv6-based current Internet architecture. The main protocol following the evolutionary approach to support the mobility is Mobile IPv6 (MIPv6), and IP Security (IPSec) for security. Both protocols have been analyzed and a lightweight version of MIPv6 with support to IPSec in order to make it suitable for the IoT ecosystems has been designed.

In addition, to the two mentioned architectures, the basis of the security and the mobility have also been addressed, a mobility detection mechanism based on movement direction determination, and the optimization of cryptographic primitives for the security protocols based on Elliptic Curve Cryptography.

In fact, the proposed communication architecture can be applied to the majority of the application sectors and markets considered for the IoT. This thesis has focused its validation for the clinical environment market.

The use cases considered are home respiratory therapy from patients with breathing problems, diabetes and drugs adherence. The drugs adherence use case has been validated with the World Health Organization [46] for Tuberculosis and a novel drugs dispenser based on the IoT has been designed and patented [47].

The proposed communication architecture has demonstrated the suitability and profitability of the IoT to build ubiquitous and mobile healthcare solutions.

Regarding other application areas, the potential of the IoT for logistic purpose in the Intelligent Transport Systems (ITS) [41, 48], Marketing [49], Smart Cities [50] and Smart Homes [51] has also been evaluated.

As a summary the list of the key contributions to the state of the art from this thesis are as follows:

- Mechanisms for addressing everything with IPv6 addressing space. On the one hand, GLoWBAL IPv6 for programmable and smart devices, and on the other hand, IPv6 Addressing Proxy for non-programmable devices inherited from legacy technologies.

- Collaboration in the optimization of the asymmetric cryptography based on ECC for constrained devices with a novel group of primes denominated Shifting Primes. This optimization has been carried out for the architectures based on the MSP430 family from Texas Instrument and the OpenRISC family (JN5139) from Jennic/NXP. In particular, this optimized asymmetric cryptography based on ECC has been integrated with IPv6-based protocols such as IPSec and the proposed communications protocols such as HIMALISEC and YOAPY.

- Design of a novel security protocol, called HIMALISEC, for the establishment and verification of trust relationships in a dynamic ecosystem with mobility support built on top of HIMALIS architecture. HIMALIS is an ID/Locator split architecture, which offers native mobility support through a clean-slate approach of the Internet architecture.

- Design and development of a lightweight version of IPSec, denominated Lightweight IPSec, for its integration with 6LoWPAN in order to support IPv6-based security for constrained devices.

- Design and development of a lightweight version of MIPv6, denominated Lightweight MIPv6, for its integration with 6LoWPAN. MIPv6 has been developed in conjunction with the mentioned Lightweight IPSec in order to offer scalable and security mobility based on IPv6.

- Design of an ad-hoc mobility protocol for critical and clinical environments, in order to offer an optimized mobility solution for scenarios where a fast handoff is required and the deployment and location of the different access points is well-known. Specifically, this protocol defines a movement detection algorithm based on Movement Direction Determination (MDD).

- Design of the interconnection framework and communication architecture for clinical environments and the determination with a group of international experts of the requirements, technologies and components involved.

- Design of a novel application protocol for clinical environments to optimize the communications in terms of delay, power consumption, bandwidth, and overhead. This protocol is denominated YOAPY, YOAPY has been designed and implemented for continuous clinical devices such as capnographer and electrocardiogram, and also for discrete clinical devices such as peak flow, spirometer, blood pressure monitor, and glucometer.

- Evaluation of the capabilities of the technology 6LoWPAN, Bluetooth Low Energy, and Near Field Communication for the continuous monitoring with the YOAPY protocol.
- Evaluation and validation of the proposed interconnection framework and communication architecture for patients with cardiovascular diseases, in the context of the Intelligent Beds (iBeds) project.
- Evaluation and validation of the proposed interconnection framework and communication architecture for patients with breathing problems, in the context of the AIRe-Health project.
- Evaluation and validation of the proposed interconnection framework and communication architecture for drugs adherence and the detection of the adverse drugs reactions.
- Finally, this interconnection framework and communication architecture has also been evaluated for diabetes, and for other scenarios out of the clinical environments scope such as Intelligent Transport Systems (ITS), Marketing, Smart Cities, and Smart Homes.

The final conclusion is that smart phones, personal data terminals, and other mobile computing devices are still far from what a future IoT will require to connect services, people, and things. But, full IPv6 integration is the first step towards this destination. As next steps one envisages support for mobility, multi-homing, discovery techniques, and management solutions in order to make things more autonomous and to enable a communications era based on the ***Future Internet of Things, Services and People***.

VI. Future works and vision

This thesis has presented the design and development of key components for contribution to the evolution of connectivity, reliability, support for heterogeneity, security and mobility.

This section describes the ongoing and future works to continue enhancing the potential of the IoT and its application in eHealth/mHealth and emerging areas such as Smart Cities.

VI.1. Towards an interoperable Internet of Things

The evolution of the IoT in order to build interoperable ecosystems is yet in progress. Figure 1.8 presents the evolution from the IoT, to the ongoing Web of Things, and to the future semantic Web of Things.

The first goal of the IoT has been to offer interconnectivity to everything, i.e. connect things to the Internet. Once connectivity is achieved we need to cope with

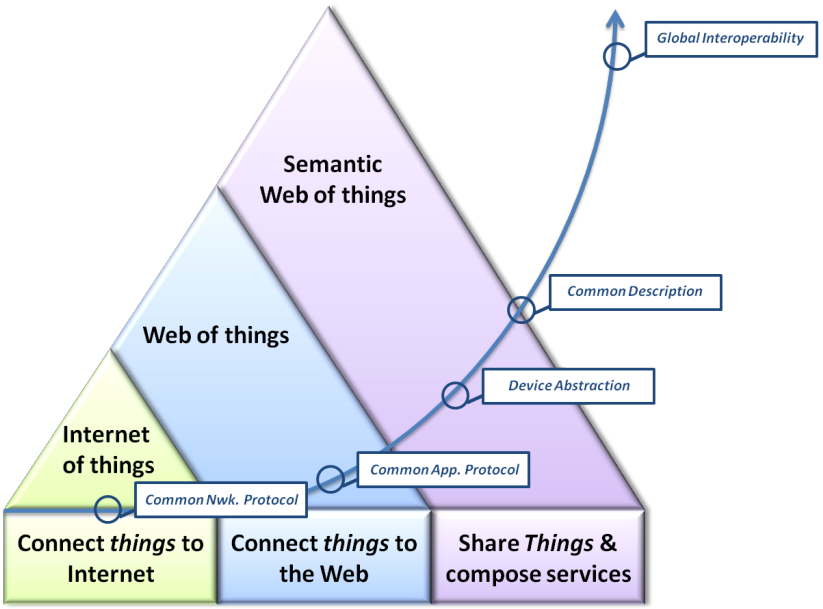


Figure 1.8: Evolution of the market size from the Internet of Things to the semantic Web of Things.

heterogeneity and enable a seamless interoperability among the different entities. For this purpose, the existing heterogeneous islands of devices have been focused on moving towards IPv6. Specifically, this integration at the connectivity level is reached with solutions such as 6LoWPAN [40], and the contributions from this thesis such as GLoWBAL IPv6 and the IPv6 Addressing Proxies. After connectivity is reached, then a common protocol for the transport and application layer is required. The most extended application in the Internet is the World Wide Web, and consequently the data transfer protocol designed for the Web, i.e., the Hypertext Transport Protocol (HTTP). The capabilities of offering an homogeneous application protocol in HTTP have been squeezed by the Web Services during the last decade. Nowadays, technologies such as Hypertext Markup Language (HTML), for the representation of resources, and JavaScript, for building logic and intelligence, are making its potential even greater. For example, HTML5 and JavaScript enable everyday desktop applications over the Web, at the same time, providing a road on which to interoperate and exchange information among different applications. For that reason, the next step in the IoT had been to connect things to the Web, thereby conceiving the so-called Web of Things.

The new protocols such as Constrained Application Protocol (CoAP) and other lightweight versions of HTTP make interaction with resources from constrained devices through Web clients such as browsers, feasible. This Web-based interaction offers to the Internet of Things the simplicity and flexibility that the Web offers nowadays.

The Web of Things is allowing different things and systems to interact together. As a result, it composes more complex services and solutions. These interactions are enabled through the definition of application programming interfaces (API) over

HTTP or CoAP protocol. Consequently, the applications give leverage to the HTTP protocol in order to provide the interface for publishing data updates into the system, for retrieving data updates from the system, and in general, exchange of information.

The data can be encoded with different envelopes, semantics and metadata. For example, the data can be encapsulated in plain text, over complex structures such as XML/EXI or simpler but yet organized structures such as JSON. In addition, they can be represented with different format and units, and finally they can offer additional information.

The current market of the IoT is focused on deployments that are connected vertically, i.e. stovepiped, to the specific sensors and applications for which they have been designed in order to address specific requirements and target a specific use case. However, the IoT requires horizontal integration of multiple capabilities and resources towards a larger ecosystem.

Therefore, IoT is not only a vehicle for communication, but also is about integration and interoperability, and to this end, semantic is the major driver.

The challenge after the Web of Things, is to build a Semantic Web of Things (SWoT) in order to ensure a common understanding as a result of which resources would be able to cooperate, be shared, linked, and combined in order to build complex services with higher intelligence and context aware. Thus, the Internet of Things will provide added value to the existing and emerging markets, which would exploit the huge potential of everything connected being controllable and providing continuously (i.e. every time) data from everywhere.

The SWoT is, on the one hand, the fusion of the trends of the IoT for moving towards Web technologies with protocols such as CoAP, REST architecture and the Web of Things concept, and on the other hand, the evolution of the Web with the Semantic Web technologies.

SWoT promises a seamless extension to the IoT allowing integration of both the physical and digital worlds. SWoT is focused on providing wide scale interoperability that allows the sharing and re-use of these things. Consequently, the use cases and markets of the IoT will not be held back to vertical solutions or pre-established use cases. In fact, these deployed infrastructures and available data can target other secondary markets and use cases, since the data that they are collecting and managing can be of importance in providing data analysis (aggregated, anonymity, processed information, e.g. for Smart City administration). They provide a major understanding of the primary markets, since they can be contrasted and extended with the available third party data.

Therefore, the challenges to move from the IoT/WoT towards the SWoT are several, some of these are to define a common description that callow data to be universally understandable create extensible annotations, i.e. from minimal semantic descriptions towards more elaborate ones, and agree on a catalogue of semantic descriptions.

These challenges can be addressed only in an ideal ecosystem, since several products will develop unique features that will be out of the scope of the existing standards and each manufacturer is associated with a different standard organization, and the standards landscape related to M2M is very large. Nowadays in numbers, the Global

Standards Collaboration Machine-Machine Task Force (GSC MSTF) identifies 143 organizations with a direct or indirect interest in M2M standardization [52].

The ongoing work looks into the convergence of the emerging standards, of the capillary and cellular networks, towards an interoperable IoT ecosystem.

First, the standards considered for cellular networks have been initialized by the European side with the ETSI M2M and extended globally with the oneM2M initiative, which is already offering the OMA Lightweight Device Management Protocol.

Second, the standards considered for capillary networks are supported by organizations such as the Internet Engineering Task Force with solutions such as CoAP, which is supported by industry alliances such as IPSO Alliance, with the IPSO OMA Web Objects Application Guidelines. The capillary networks present major heterogeneity and other standards for offering a lightweight reliable messaging transport protocol for the IoT such as the Message Queuing Telemetry Transport (MQTT) protocol. This protocol is optimized to connect physical world devices and events with enterprise servers and other consumers supported by OASIS and Eclipse Foundation [53], and other private standards such as the ZigBee-IP solution for Smart Energy (SE 2.0) supported by the ZigBee Alliance [22].

Other activities and projects are the W3C with the SSN-XG ontology for offering a semantic layer for the IoT, the European Research Cluster on the Internet of Things (IERC), and its projects such as OpenIoT, IoT.est, and SPITFIRE where the capabilities of RDF, OWL and classic semantic technologies for the IoT have been explored.

Since the current environment regarding semantic is quite fuzzy, the future work requires reaching a more homogeneous and clear standards ecosystem, where the manufacturers and vendors can determine what to apply to where in the different IoT use cases.

VI.2. Towards a distributed trust and security

This thesis has presented the optimization cryptographic primitives for asymmetric key cryptography based on Elliptic Curve Cryptography (ECC), lightweight design and development of IPSec for the support of security over IPv6, and finally HIMALISEC for the distributed trust and security management over ID/Locator split architectures.

The ongoing work is focused on solutions to carry out IoT/M2M trust verification, through a mechanism such as capabilities-based access control. Consequently, novel scenarios based on temporal access to resources can be defined. For example, a house proprietor with an access control solution (e.g. a smart door lock) is able to offer temporal access to his neighbor so as to go everyday at anytime from 15:00 to 18:00 in order to feed the pets and irrigate the plants.

The mechanisms required to offer secure solutions that make usage of the IoT capabilities feasible during usual human activities and behaviors, where devices and physical resources are involved, needs to be enhanced. As a result, these new mechanisms and solutions will facilitate the introduction of the IoT as part of the Internet-powered society.

The communications between IoT-devices and humans present two different ways to be satisfied, the first, an integration of the required communication technologies and capabilities in personal devices such as Smart Phones. Following this approach, the potential of WiFi Low Power, Bluetooth Low Energy, and Near Field Communication could be exploited. Thus, the smart object can talk with the personal device through the same medium technologies, i.e. WiFi Low Power, Bluetooth Low Energy, etc. However this approach presents high requirements such as compatibility in the medium technology between the personal device and the smart object. Consequently it is limiting the availability and success of these solutions.

For that reason, the other approach is the exploitation of the common and abstracted communication medium with IP technology. In this case, the personal device and the objects can be connected to the Internet through any communication interface, and communication between them is based on the end-to-end feature of the IP technology. As a result, it is not required that the smart object and the personal device use similar technology to establish the communication.

These distributed security scenarios, based on both IP abstracted technology and direct interaction, are being explored with the techniques such as the capability-based token mentioned.

VI.3. Towards a ubiquitous and mobile Internet of Things

IoT and M2M are being enabled and developed from the capillary and the cellular points of view. This thesis has explored and enabled a mobile IoT for the capillary networks with the lightweight Mobile IPv6 protocol.

However, a mobile IoT based on cellular networks to also provide ubiquitous access and mobility between different networks can also be defined.

The mobile IoT based on capillary networks present challenges in terms of the availability of coverage in a wide scale, and the lack of agreements among different network access providers involved.

For that reason, the IoT based on cellular networks perspective is also gaining attention, since this provides a wider range of coverage, and homogeneous technology worldwide (regulated by the 3GPP Alliance). In particular, the last version of the Long Term Evolution-Advanced (LTE-A) standard defines how to integrate IoT/M2M devices.

The inconvenience of the cellular networks continue to be the requirement of a subscription (i.e. dependence with a network access provide), higher power consumption, and higher costs.

For that reason, mobility protocols with vertical handoff among different technologies, i.e. between capillary and cellular networks need to be explored, in order to provide the best trade-off in terms of communication costs, availability and reliability.

These kind of signaling protocols between cellular and capillary networks are becoming a reality, thanks to the convergence of both with the Open Mobile Alliance (OMA) Lightweight Device Management Protocol (LWM2M).

Therefore, a set of objects for the mobility-related signaling can be defined, which can be supported by the solutions promoted from the cellular vendors and manufacturers (i.e. oneM2M Alliance), and from the capillary vendors and manufacturers (i.e. IPSO Alliance).

VI.4. Towards a valuable Internet of Things

Finally, the major challenge for the Internet of Things is to demonstrate its value to the end-customers.

The potential of the end-to-end connectivity and convergence with the Internet and Web protocols are providing, from the developing and engineering perspective, highly valuable advantages.

Some of these advantages are the reduction of costs for the development of solutions thanks to the re-usage of existing technologies; major interoperability thanks to common communications technology; major control and monitoring capabilities; a major number of possibilities to compose services based on cybernetic and physical resources, and major flexibility.

However, even when this list of advantages could be considered sufficient motivation to justify the value of the IoT, it continues to not be enough from the consumers perspective, since none of them are directly related to perceptible values by the end user.

All of them provide big opportunities to develop and offer a solution that can breakthrough the market. However, the killer solutions or applications based on the IoT, which demonstrate to the consumers the potential of the IoT, are yet to come.

In my opinion, the two trends to build this value powered by the IoT potential can be based on an evolve approach, or in a totally novel value proposal.

Regarding the evolve approach, the IoT can offer the same solutions that nowadays are being offered by existing technologies but with major simplicity for usage, interaction and understanding. For example, current industrial automation solutions (e.g., SCADA) are featured by a complex set-up process, where a set of skills and training is required. The potential of the IoT is to set-up these physical devices through more understandable platforms such as smart phones, remotely through Internet-based solutions, and even automatic configuration based on the smart capabilities of smart objects to come. For example, some of their smart capabilities are the potential to discover other devices, exchange messages with control and monitoring systems, and set-up automatically a big part of the conventionally required parameters.

An example of this approach is what our ongoing work is offering with the developed Smart Driver for lighting in Smart Cities. The Smart Driver is featured by being a power supplier with Internet connectivity and processing capabilities. These new two features offer the potential to set-up current, voltage, and logic scheduling directly from any IP-enabled device without requiring the set-up with specific and complex solutions, while the device is connected to a proprietary software or device.

The other approach is to offer a novel value proposal, which is inspired in the potential of the data. One of the advantages of this new capability to connect with

everything is the potential capability to collect data from everything in a major frequency on a temporary basis. Consequently, this data with proper data mining, a.k.a. Big Data tools, will offer solutions that were not feasible before.

For instance, following the example of street lighting, the data gathered from each street light is not limited to the control of the street light, it can also offer additional data from humidity, temperature, nose, quality of air, motion, etc. Thus, novel solutions such as noisy maps and pollution maps can be built to evaluate the quality in the different zones before renting or buying a house.

In addition to the sensors that can been integrated in the Smart Driver itself, these Smart Objects present endless possibilities, since they can be also seen as the infrastructure to connect and communicate to any device.

Therefore, the integration of the Internet and IoT-related capabilities in a street light that initially could be motivated to optimize power consumption, simplify the set-up, and enable the remote and monitoring platforms, is also converted into a big opportunity to build a nerve for the rest of the devices. This nerve can provide connectivity to the parking pots, citizens' devices, cars, gardens, and in short, any of the entities that are part of the city ecosystem.

The smart lighting solution described for smart cities pursue the goal of offering major power consumption reduction, and a major awareness about air and acoustical pollution in order to carry out the proper actions to enhance sustainability.

Another example based on eHealth/mHealth is the interconnection among different devices. For example, for patients with diabetes type 1, devices for Continuous Glucose Monitoring (GCM) and also insulin pumps to provide the insulin therapy are provided nowadays.

These devices are starting to be able to interact between each other, but without any action, only to show the data to the user, due to the lack of intelligence in both them.

IoT enables the insulin pump and the GCM to interact with intelligence devices such as a smart phone, swatch, and even with a backend system deployed in the cloud that can offer a calculus of the insulin therapy based on the patient's health record, evolution, and in short Big Data from the patient. Consequently, the loop between monitoring, therapy and user can be closed in a smarter and simpler way, and consequently avoid that the user needs to introduce manually the insulin dosage in the insulin pump multiple times per day.

These mHealth-based solutions pursue the goal of offering to patients with chronic diseases a major level of freedom with respect to their illness, and quality of life. All these new interaction models, knowledge, and improvement of the existing solutions are some of the ways that we can start building and probing the value of the IoT. In short, the IoT is another enabler to continue improving both quality of life and experiences, and planet sustainability.

Chapter 2

Interconnection framework for mHealth and remote monitoring based on the Internet of Things

Title:	Interconnection framework for mHealth and remote monitoring based on the Internet of Things
Authors:	Antonio J. Jara, Miguel A. Zamora, Antonio F. Skarmeta
Journal:	IEEE Journal on Selected Areas in Communications (J-SAC)
ISSN:	0733-8716
Impact factor:	3,413 (2011) - Position 4 out of 79 (See section I)
Publisher:	IEEE
Volume:	31
Number:	9
Pages:	47-65
Year:	2013
Month:	August
DOI:	10.1109/JSAC.2013.SUP.0513005
Link:	`http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6585881`
State:	Published

Abstract: *Communication and information access defines the basis to reach a personalized health end-to-end framework. Personalized health capability is limited to the available data from the patient. It is usually dynamic and incomplete. Therefore, it presents a critical issue for mining, analysis and trending. For that reason, this work presents an interconnection framework for mobile Health (mHealth) based on the Internet of Things. It makes continuous and remote vital sign monitoring feasible. It introduces technological innovations for empowering health monitors and patient devices with Internet capabilities. It allows patient monitoring and supervision by remote centers, and personal platforms such as tablets. From the hardware point of view, it offers a gateway and a personal clinical device used for the wireless transmission of continuous vital signs through 6LoWPAN, and patient identification through RFID. From the software point of view, this interconnection framework presents a novel protocol, called YOAPY, for an efficient, secure, and scalable integration of the sensors deployed in the patient's personal environment. This paper presents the architecture, and evaluates its capabilities to provide continuous monitoring, ubiquitous connectivity, extended device integration, reliability, and support for security and privacy. The proposed interconnection framework and the proposed protocol for the sensors has been exhaustively evaluated in the framework of the AIRE project, which is focused on patients with breathing problem. This evaluates for the proposed protocol the data aggregation mechanism level, Round-Trip delay Time, impact of the distance, and the impact of the security. It has been concluded that secure continuous monitoring is feasible with the use of the proposed YOAPY aggregation mechanisms, and the capabilities from the proposed interconnection framework.*

Chapter 3

Extending the Internet of Things to the Future Internet through IPv6 support

Title:	Extending the Internet of Things to the Future Internet through IPv6 support
Authors:	Antonio J. Jara, Socrates Varakliotis, Antonio F. Skarmeta, Peter Kirstein
Journal:	Mobile Information Systems
ISSN:	Print (1574-017x) Online (1875-905X)
Impact factor:	2,432 (2011) - Position 8 out of 79 (See section II)
Publisher:	IOS Press
Volume:	9
Year:	2013
Month:	July
DOI:	10.3233/MIS-130169
Link:	`http://iospress.metapress.com/content/wgj522g068321467/`
State:	Published

Abstract: *Emerging Internet of Things (IoT)/Machine-to-Machine (M2M) systems require a transparent access to information and services through a seamless integration into the Future Internet. This integration exploits infrastructure and services found on the Internet by the IoT. On the one hand, the so-called Web of Things aims for direct Web connectivity by pushing its technology down to devices and smart things. On the other hand, the current and Future Internet offer stable, scalable, extensive, and tested protocols for node and service discovery, mobility, security, and auto-configuration, which are also required for the IoT. In order to integrate the IoT into the Internet, this work adapts, extends, and bridges using IPv6 the existing IoT building blocks (such as solutions from IEEE 802.15.4, BT-LE, RFID) while maintaining backwards compatibility with legacy networked embedded systems from building and industrial automation. Specifically, this work presents an extended Internet stack with a set of adaptation layers from non-IP towards the IPv6-based network layer in order to enable homogeneous access for applications and services.*

Chapter 4

GLoWBAL IP: An adaptive and transparent IPv6 integration in the Internet of Things

Title:	GLoWBAL IP: An adaptive and transparent IPv6 integration in the Internet of Things
Authors:	Antonio J. Jara, Miguel A. Zamora, Antonio F. Skarmeta
Journal:	Mobile Information Systems
ISSN:	Print (1574-017x) Online (1875-905X)
Impact factor:	2,432 (2011) - Position 8 out of 79 (See section II)
Publisher:	IOS Press
Volume:	8
Number:	3
Pages:	177-197
Year:	2012
DOI:	10.3233/MIS-2012-0138
Link:	`http://iospress.metapress.com/content/x611r3t20n171102`
State:	Published

Abstract: *The Internet of Things (IoT) requires scalability, extensibility and a transparent integration of multi-technology in order to reach an efficient support for global communications, discovery and look-up, as well as access to services and information. To achieve these goals, it is necessary to enable a homogenous and seamless machine-to-machine (M2M) communication mechanism allowing global access to devices, sensors and smart objects. In this respect, the proposed answer to these technological requirements is called Glowbal IP, which is based on a homogeneous access to the devices/sensors offered by the IPv6 addressing and core network. Glowbal IP's main advantages with regard to 6LoWPAN/IPv6 are not only that it presents a low overhead to reach a higher performance on a regular basis, but also that it determines the session and identifies global access by means of a session layer defined over the application layer. Technologies without any native support for IP are thereby adaptable to IP e.g. IEEE 802.15.4 and Bluetooth Low Energy. This extension towards the IPv6 network opens access to the features and methods of the devices through a homogenous access based on WebServices (e.g. RESTFul/CoAP). In addition to this, Glowbal IP offers global interoperability among the different devices, and interoperability with external servers and users applications. All in all, it allows the storage of information related to the devices in the network through the extension of the Domain Name System (DNS) from the IPv6 core network, by adding the Service Directory extension (DNS-SD) to store information about the sensors, their properties and functionality. A step forward in network-based information systems is thereby reached, allowing a homogenous discovery, and access to the devices from the IoT. Thus, the IoT capabilities are exploited by allowing an easier and more transparent integration of the end users applications with sensors for the future evaluations and use cases.*

Chapter 5

IPv6 addressing Proxy: Mapping native addressing from legacy technologies and devices to the Internet of Things (IPv6)

Title:	IPv6 addressing Proxy: Mapping native addressing from legacy technologies and devices to the Internet of Things (IPv6)
Authors:	Antonio J. Jara, Pedro Moreno-Sanchez, Antonio F. Skarmeta, Socrates Varakliotis, Peter Kirstein
Journal:	Sensors
ISSN:	1424-8220
Impact factor:	1,739 (2011) - Position 14 out of 58 (See section III)
Publisher:	Multidisciplinary Digital Publishing Institute (MDPI)
Volume:	13
Number:	5
Pages:	6687-6712
Year:	2013
Month:	May
DOI:	10.3390/s130506687
Link:	`http://www.mdpi.com/1424-8220/13/5/6687`
State:	Published

Abstract: *Sensors utilize a large number of heterogeneous technologies for a varied set of application environments. The sheer number of devices involved requires that this Internet be the Future Internet, with a core network based on IPv6 and a higher scalability in order to be able to address all the devices, sensors and things located around us. This capability to connect through IPv6 devices, sensors and things is what is defining the so-called IoT. IPv6 provides addressing space to reach this ubiquitous set of sensors, but legacy technologies, such as X10, EIB, CAN and RFID, do not support IPv6 protocol. For that reason, a technique must be devised to map the sensor and identification technologies to IPv6. This paper proposes a mapping between the native addressing of each technology and an IPv6 address following a set of rules which are discussed and proposed in this work. Specifically, the paper presents a technology-dependent IPv6 addressing proxy, which maps each device to the different sub-networks built under the IPv6 prefix addresses provided by the Internet Service Provider for each home, building or user. The IPv6 addressing proxy offers a common addressing environment based on IPv6 for all the devices regardless of the device technology. Thereby, this offers a scalable and homogeneous solution to interact with devices which do not support IPv6 addressing. The IPv6 addressing proxy has been implemented in a multi-protocol card, and evaluated successfully its performance, scalability and interoperability through a protocol built over IPv6.*

Chapter 6

Shifting primes: Optimizing elliptic curve cryptography for 16-bit devices without hardware multiplier

Title:	Shifting primes: Optimizing elliptic curve cryptography for 16-bit devices without hardware multiplier
Authors:	Leandro Marin, Antonio J. Jara, Antonio F. Skarmeta
Journal:	Mathematical and Computer Modelling
ISSN:	0895-7177
Impact factor:	1,346 (2011) - Position 24 out of 104 (See section IV)
Publisher:	ELSEVIER
Volume:	58
Number:	5-6
Pages:	1155–1174
Year:	2013
Month:	September
DOI:	10.1016/j.mcm.2013.02.008
Link:	`http://www.sciencedirect.com/science/article/pii/S0895717713000563`
State:	Published

Abstract: *Security for the Internet of Things (IoT) presents the challenge of offering suitable security primitives to enable IP-based security protocols such as IPSec and DTLS. This challenge is here because host-based implementations and solutions are not providing a proper performance over the devices used in the IoT. This is mainly because of the use of highly constraint devices in terms of computational capabilities. Therefore, it is necessary to implement new optimized and scalable cryptographic primitives which can use existing protocols to provide security, authentication, privacy and integrity to the communications. Our research focuse on the mathematical optimization of cryptographic primitives for Public Key Cryptography (PKC) based on Elliptic Curve Cryptography (ECC). PKC has been considered, since the IoT requires high scalability, multi-domain interoperability, self-commissioning, and self-identification. Specifically, this contribution presents a set of optimizations for ECC over constrained devices, and a brief tutorial of its implementation in the microprocessor Texas Instrument MSP430 (commonly used in IoT devices such as 6LoWPAN, active RFID and DASH7). Our main contribution is the proof that these special pseudo-Mersenne primes, which we have denominated 'shifting primes' can be used for ECC primitives with 160-bit keys in a highly optimal way. This paper presents an ECC scalar multiplication with 160-bit keys within 5.4 million clock cycles over MSP430 devices without hardware multiplier. Shifting primes provide a set of features, which make them more compliant with the set of instructions available with tiny CPUs such as the MSP430 and other 8 and 16-bit CPUs.*

Chapter 7

Secure and Scalable Mobility Management Scheme for the Internet of Things Integration in the Future Internet Architecture

Title:	Secure and Scalable Mobility Management Scheme for the Internet of Things Integration in the Future Internet Architecture
Authors:	Antonio J. Jara, Ved P. Kafle, Antonio F. Skarmeta
Journal:	International Journal of Ad Hoc and Ubiquitous Computing
ISSN:	Print (1743-8225) Online (1743-8233)
Impact factor:	0,848 (2011) - Position 47 out of 79 (See section VI)
Publisher:	Inderscience Publishers
Volume:	13
Number:	3-4
Pages:	228-242
Year:	2013
DOI:	10.1504/IJAHUC.2013.055468
Link:	`http://www.inderscience.com/info/inarticle.php?artid=55468`
State:	Published

Abstract: *Internet of Things is becoming a reality with the rapid development of communication technologies. This evolution presents an enrichment of the users' experiences, but also challenges regarding network scalability, security, privacy vulnerabilities, and mobility support. Mobility support for the Future Internet is focused on ID/Locator split architectures since the limitations of the current Internet. This work analyzes the security challenges for the HIMALIS (Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation) architecture for the particularities from the Internet of Things and the ID/Locator management messages vulnerable to attacks. This work proposes a secure and scalable mobility management scheme that considers the constraints from the Internet of Things, solving the possible security and privacy vulnerabilities of the HIMALIS architecture. The proposed scheme supports scalable inter-domain authentication and secure location update and binding transfer for the mobility process. The proposed scheme has been verified and evaluated successfully with the AVISPA framework.*

Chapter 8

Lightweight MIPv6 with IPSec support

Title:	Lightweight MIPv6 with IPSec support: A mobility protocol for enabling transparent IPv6 mobility in the Internet of Things with support to the security
Authors:	Antonio J. Jara, David Fernandez, Pablo Lopez, Miguel A. Zamora, Antonio F. Skarmeta
Journal:	Mobile Information Systems
ISSN:	Print (1574-017x) Online (1875-905X)
Impact factor:	2,432 (2011) - Position 8 out of 79 (See section II)
Publisher:	IOS Press
Volume:	9
Year:	2013
Month:	July
DOI:	10.3233/MIS-2012-0138
Link:	`http://iospress.metapress.com/content/n82j053850436262/`
State:	Published

Abstract: *Mobility management is a desired feature for the emerging Internet of Things (IoT). Mobility aware solutions increase the connectivity and enhance adaptability to changes of the location and infrastructure. IoT is enabling a new generation of dynamic ecosystems in environments such as smart cities and hospitals. Dynamic ecosystems require ubiquitous access to Internet, seamless handover, flexible roaming policies, and an interoperable mobility protocol with existing Internet infrastructure. These features are challenges for IoT devices, which are usually constrained devices with low memory, processing, communication and energy capabilities. This work presents an analysis of the requirements and desirable features for the mobility support in the IoT, and proposes an efficient solution for constrained environments based on Mobile IPv6 and IPSec. Compatibility with IPv6-existing protocols has been considered a major requirement in order to offer scalable and inter-domain solutions that were not limited to specific application domains in order to enable a new generation of application and services over Internet-enabled dynamic ecosystems, and security support based on IPSec has been also considered, since dynamic ecosystems present several challenges in terms of security and privacy. This work has, on the one hand, analysed suitability of Mobile IPv6 and IPSec for constrained devices, and on the other hand, analysed, designed, developed and evaluated a lightweight version of Mobile IPv6 and IPSec. The proposed solution of lightweight Mobile IPv6 with IPSec is aware of the requirements of the IoT and presents the best solution for dynamic ecosystems in terms of efficiency and security adapted to IoT-devices capabilities. This presents concerns in terms of higher overhead and memory requirements. But, it is proofed and concluded that even when higher memory is required and major overhead is presented, the integration of Mobile IPv6 and IPSec for constrained devices is feasible.*

Chapter 9

Mobile IP-Based Protocol for WPANs in Critical Environments

Title:	Mobile IP-Based Protocol for WPANs in Critical Environments
Authors:	Antonio J. Jara, Ricardo M. Silva, Jorge S. Silva, Miguel A. Zamora, Antonio F. Skarmeta
Journal:	Wireless Personal Communications
ISSN:	Print (0929-6212) Online (1572-834X)
Impact factor:	0,458 (2011) - Position 60 out of 79 (See section V)
Publisher:	Springer US
Volume:	61
Number:	4
Pages:	711-737
Year:	2011
Month:	December
DOI:	10.1007/s11277-011-0428-y
Link:	`http://link.springer.com/10.1007/s11277-011-0428-y`
State:	Published

Abstract: *Low-power Wireless Personal Area Networks (LoWPANs) are still in their early stage of development, but the range of conceivable usage scenarios and applications is tremendous. That range is extended by its inclusion in Internet with IPv6 Low-Power Personal Area Networks (6LoWPANs). This makes it obvious that multi-technology topologies, security and mobility support will be prevalent in 6LoWPAN. Mobility based communication increases the connectivity, and allows extending and adapting LoWPANs to changes in their location and environment infrastructure. However, the required mobility is heavily dependent on the individual service scenario and the LoWPAN architecture. In this context, an optimized solution is proposed for critical applications, such as soldier health monitoring, fire rescue or healthcare, where people need to frequently change their position. Our scenario is health monitoring in an oil refinery where many obstacles have found to the effective use of LoWPANs in these scenarios, mainly due to transmission medium features i.e. high losses, high latency and low reliability. Therefore, it is very difficult to provide continuous health monitoring with stringent requirements on mobility. In this paper, it is proposed a paradigm for mobility over 6LoWPAN for critical environments. On the one hand the intra-mobility is supported by GinMAC, which is an extension of IEEE 802.15.4 to support a topology control algorithm, which offers intra-mobility transparently, and Movement Direction Determination (MDD) of the Mobile Node (MN). On the other hand, the inter-mobility is based on pre-set-up of the network parameters in the visited networks, such as Care of Address and channel, to reach a fast and smooth handoff. Pre-set-up is reached since MDD allows discovering the next 6LoWPAN network towards which MN is moving. The proposed approach has been simulated, prototyped, evaluated, and is being studied in a scenario of wearable physiological monitoring in hazardous industrial areas, specifically oil refineries, in the scope of the GinSeng European project.*

Chapter 10

Evaluation of Bluetooth Low Energy capabilities for tele-mobile monitoring in home-care

Title:	Evaluation of Bluetooth Low Energy capabilities for tele-mobile monitoring in home-care
Authors:	Antonio J. Jara, Pablo Lopez, David Fernandez, Miguel A. Zamora, Antonio F. Skarmeta, Leandro Marin
Journal:	Journal of Universal Computer Science (J.UCS)
ISSN:	Print (0948-695x) Online (0948-6968)
Impact factor:	0,669 (2011) - Position 85 out of 104 (See section IX)
Publisher:	Graz University of Technology
Volume:	19
Number:	9
Pages:	1219-1241
Year:	2013
Month:	May
Link:	`http://www.jucs.org/jucs_19_9/evaluation_of_bluetooth_low`
State:	Published

Abstract:

Bluetooth Low Energy (BT-LE) is extending Bluetooth technology to devices with lower communication requirements and higher constraints in terms of memory capabilities and power autonomy. Thereby, BT-LE makes feasible the wireless transmission of information from smart objects such as wearable clinical devices, ambient sensors and actuators. These smart objects are starting to be internet-enabled devices, reaching the so denominated Internet of Things (IoT). Our research work is focused on analyze the capabilities of these technologies for continuous data transmission and integration of clinical sensors in home-care and Ambient Assisted Living environments. For this purpose, this work analyzes exhaustively the capabilities from BT-LE and compare this with the capabilities from Bluetooth 2.1. In addition, it has been considered the communications requirements from different clinical devices such as an electrocardiogram (ECG) and a capnograph. It is concluded that the performance from BT-LE is lower than Bluetooth Classic (Bluetooth 2.1), since its limitations to be based on datapoints instead of P2P communications. Therefore, it is necessary to perform data compression/aggregation when the amount of data to send is too large. This work also presents how to apply pre-processing techniques that greatly reduces the transmission overload (performs signal compression) in order to allow the continuous transmission of the ECG and capnograph signal through BT-LE making so feasible the integration of continuous clinical devices via BT-LE.

Chapter 11

Communication protocol for enabling continuous monitoring of elderly people through NFC

Title:	Communication protocol for enabling continuous monitoring of elderly people through Near Field Communications
Authors:	Antonio J. Jara, Pablo Lopez, David Fernandez, Miguel A. Zamora, Benito Ubeda, Antonio F. Skarmeta
Journal:	Interacting with Computers
ISSN:	Print (0953-5438) Online (1873-7951)
Impact factor:	1,233 (2011) - Position 8 out of 20 (See section VIII)
Publisher:	Oxford Journals
Volume:	25
Year:	2013
Month:	May
DOI:	10.1093/iwc/iwt030
Link:	`http://iwc.oxfordjournals.org/content/early/2013/05/15/iwc.iwt030.abstract?keytype=ref&ijkey=zf2XrSpVFk3fPML`
State:	Published

Abstract: *Continuous and wireless transmission of vital signs for personalized healthcare is gaining a great deal of interest from AAL solutions. Personalized Healthcare capabilities are limited to the patient data available, which is usually dynamic and incomplete. For that reason, regular monitoring of patients with the aim of offering a suitable analysis of patient evolution is required. Continuous monitoring requires the integration of wireless communication technologies and embedded systems into wearable and portable monitoring systems. In addition, a user interface intuitive is also required, that is easy to use and that the patients and caregivers can understand. This work proposes a solution such as NFC for personalized healthcare based on the IoT. NFC is a technology integrated in smart phones that provides capabilities for identification of devices/sensors, and presents ubiquitous communication capabilities between sensor and device. NFC also presents challenges in terms of the performance and efficiency of data transmission, due to the constrained resources and capabilities of ubiquitous devices and the latency introduced by the NFC technology. This paper presents a novel monitoring system for continuous data transmission from a set of clinical devices based on NFC which has been optimized in order to make communications feasible. This novel monitoring system is also composed by a set of participatory sensing applications to support caregivers and for patients to self-monitor and self-manage their health status wirelessly. A technical evaluation based on latencies associated with use of NFC for continuous monitoring and an evaluation of usability by a group of elderly users and their caregivers, that studies the interactions between the users and the system, are demonstrated.*

Chapter 12

Drug identification and interaction checker based on IoT to minimize adverse drug reactions and improve drug compliance

Title:	Drug identification and interaction checker based on IoT to minimize adverse drug reactions and improve drug compliance
Authors:	Antonio J. Jara, Miguel A. Zamora, Antonio F. Skarmeta
Journal:	Personal and Ubiquitous Computing
ISSN:	Print (1617-4909) Online (1617-4917)
Impact factor:	0,938 (2011) - Position 67 out of 135 (See section VII)
Publisher:	Springer-Verlag
Year:	2012
Month:	October
DOI:	10.1007/s00779-012-0622-2
Link:	`http://link.springer.com/article/10.1007/s00779-012-0622-2`
State:	Published

Abstract:

Drug compliance and adverse drug reactions (ADR) are two of the most important issues regarding patient safety throughout the worldwide healthcare sector. ADR prevalence is 6.7 % throughout hospitals worldwide, with an international death rate of 0.32 % of the total of the patients. This rate is even higher in Ambient Assisted Living environments, where 15 % of the patients suffer clinically significant interactions due to patient non-compliance to drug dosage and schedule of intake in addition to suffering from polypharmacy. These instances increase with age and cause risks of drug interactions, adverse effects, and toxicity. However, with a tight follow-up of the drug treatment, complications of incorrect drug use can be reduced. For that purpose, we propose an innovative system based on the Internet of Things (IoT) for the drug identification and the monitoring of medication. IoT is applied to examine drugs in order to fulfill treatment, to detect harmful side effects of pharmaceutical excipients, allergies, liver/renal contradictions, and harmful side effects during pregnancy. The IoT design acknowledges that the aforementioned problems are worldwide so the solution supports several IoT identification technologies: barcode, Radio Frequency Identification, Near Field Communication, and a new solution developed for low-income countries based on IrDA in collaboration with the World Health Organization. These technologies are integrated in personal devices such as smart-phones, PDAs, PCs, and in our IoT-based personal healthcare device called Movital.

Bibliography

[1] Thomson Reuters, "Journal citation reports", 2011, `http://thomsonreuters.com/products_services/science/science_products/a-z/journal_citation_reports/`.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey", *Computer Networks*, vol. Vol. 54, no. no. 15, pp. pp. 2787–2805, 2010.

[3] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless-and mobility-related view", *IEEE Wireless Communications*, vol. Vol. 17, no. no. 6, pp. pp. 44–51, 2010.

[4] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the internet of things", *IEEE Internet Computing*, vol. Vol. 14, no. no. 1, pp. pp. 44–51, 2010.

[5] Zach Shelby, Klaus Hartke, and Carsten Bormann, "Constrained application protocol (coap)", 2013, `http://tools.ietf.org/html/draft-ietf-core-coap-14`.

[6] J. FroehlichJon, J. Neumann, and N. Oliver, "Measuring the pulse of the city through shared bicycle programs", *Proc. of UrbanSense08*, pp. pp. 16–20, 2008.

[7] Laura DeNardis, "Standards and ehealth: Itu-t technology watch report", Tech. Rep., ITU-T, 2011.

[8] Antonio J. Jara, Miguel A. Zamora, and Antonio F. Skarmeta, "A wearable system for tele-monitoring and tele-assistance of patients with integration of solutions from chronobiology for prediction of illness", *Ambient Intelligence and Smart Environments*, vol. 1 - Ambient Intelligence Perspectives, 2008, 10.3233/978-1-58603-946-2-221.

[9] R.S.H. Istepanian, A. Jara, A. Sungoor, and N. Philips, "Internet of things for m-health applications (iomt)", in *AMA IEEE Medical Tech. Conf. on Individualized Healthcare*, 2010, Washington (USA).

[10] Antonio J. Jara, Miguel A. Zamora, and Antonio F. Skarmeta, "An internet of things–based personal device for diabetes therapy management in ambient assisted living (aal)", *Personal and Ubiquitous Computing*, vol. Vol. 15, no. no. 4, pp. pp. 431–440, 2011, DOI: 10.1007/s00779-010-0353-1.

[11] A. Dohr, "The internet of things for ambient assisted living", in *Seventh International Conference on Information Technology*, 2010, pp. pp. 804–809, ITNG.

[12] Chung-Chih Lin, Ming-Jang Chiu, Chun-Chieh Hsiao, Ren-Guey Lee, and Yuh-Show Tsa, "Wireless health care service system for elderly with dementiag", *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, pp. pp. 696–704, 2006.

[13] James Middleton, "Doctor who", 2011, `http://www.telecoms.com/29938/doctor-who/`.

[14] Zhong Fan and Siok Tan, "M2m communications for e-health: Standards, enabling technologies, and research challenges", in *6th IEEE International Symposium on Medical Information and Communication Technology (ISMICT)*. IEEE, 2012, pp. pp. 1–4.

[15] Miguel Galarraga, Luis Serrano, Ignacio Martínez, Paula de TOLEDO, et al., "Standards for medical device communication: X73 poc-mdc", *Studies in health technology and informatics*, vol. 121, pp. 242, 2006.

[16] Randy Carroll, Rick Cnossen, Mark Schnell, and David Simons, "Continua: An interoperable personal healthcare ecosystem", *IEEE Pervasive Computing*, vol. 6, no. 4, pp. pp. 90–94, 2007.

[17] ZigBee Alliance, "Zigbee specification", *ZigBee Document 053474r13*, pp. pp. 344–346, 2006.

[18] Adam Dunkels and JP Vasseur, "Ip for smart objects", *IPSO Alliance White paper*, vol. 1, 2008.

[19] JP Vasseur, Cisco Paul Bertrand, Founder Watteco, Bernard Aboussouan, VP Marketing, Gainspan Eric Gnoske, Atmel Kris Pister, et al., "A survey of several low power link layers for ip smart objects", *Internet Protocol for Smart Objects (IPSO) Alliance*, 2010.

[20] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*, Wiley, 2009.

[21] Rafa Marin-Lopez, Fernando Pereniguez-Garcia, Antonio F Gomez-Skarmeta, and Yoshihiro Ohba, "Network access security for the internet: protocol for carrying authentication for network access", *IEEE Communications Magazine*, vol. 50, no. 3, pp. pp. 84–92, 2012.

[22] Don Sturek, "Zigbee ip stack overview", 2009, ZigBee Alliance.

[23] Shahid Raza, Simon Duquennoy, Joel Höglund, Utz Roedig, and Thiemo Voigt, "Secure communication for the internet of things—a comparison of link-layer security and ipsec for 6lowpan", *Security and Communication Networks*, 2012.

[24] Shahid Raza, Thiemo Voigt, and Vilhelm Jutvik, "Lightweight ikev2: A key management solution for both the compressed ipsec and the ieee 802.15. 4 security", in *Proceedings of the IETF Workshop on Smart Object Security*, 2012.

[25] Eric Rescorla and Nagendra Modadugu, "Rfc 6347: Datagram transport layer security version 1.2", *IETF*, 2012.

[26] Pin Nie, Juho Vähä-Herttua, Tuomas Aura, and Andrei Gurtov, "Performance analysis of hip diet exchange for wsn security establishment", in *Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks*. ACM, 2011, pp. pp. 51–56.

[27] Dino Farinacci, Darrel Lewis, David Meyer, and Vince Fuller, "Rfc 6830: The locator/id separation protocol (lisp)", *IETF*, 2013.

[28] Ved P Kafle and Masugi Inoue, "Himalis: Heterogeneity inclusion and mobility adaptation through locator id separation in new generation network", *IEICE transactions on communications*, vol. 93, no. 3, pp. pp. 478–489, 2010.

[29] Antonio J Jara, Miguel A Zamora, and Antonio Skarmeta, "Glowbal ip: An adaptive and transparent ipv6 integration in the internet of things", *Mobile Information Systems*, vol. 8, no. 3, pp. pp. 177–197, 2012.

[30] Antonio J Jara, Pedro Moreno, Antonio Skarmeta, Socrates Varakliotisy, and Peter Kirstein, "Ipv6 addressing proxy: Mapping native addressing from legacy communication technologies and protocols to ipv6 and the internet of things", in *IEEE International Conference on the Internet of Things (IoT 2012)*. IEEE, 2012, pp. pp. 1–6.

[31] Antonio J Jara, Pedro Moreno, Antonio Skarmeta, Socrates Varakliotisy, and Peter Kirstein, "Ipv6 addressing proxy: Mapping native addressing from legacy technologies and devices to the internet of things (ipv6)", *Sensors*, 2013.

[32] An Liu and Peng Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks", in *Information Processing in Sensor Networks, 2008. IPSN'08. International Conference on*. IEEE, 2008, pp. pp. 245–256.

[33] Leandro Marin, Antonio J Jara, and Antonio Skarmeta, "Shifting primes on openrisc processors with hardware multiplier", in *Information and Communication Technology, Lecture Notes in Computer Science (LNCS)*, pp. pp. 540–549. Springer, 2013.

[34] George Roussos and Paul Chartier, "Scalable id/locator resolution for the iot", in *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, 2011, pp. pp. 58–66.

[35] AJ Jara, Ricardo M Silva, Jorge Silva, MA Zamora, and AFG Skarmeta, "Mobile ipv6 over wireless sensor networks (6lowpan) issues and feasibility", *European Wireless Sensor Networks (EWSN)*, 2010.

[36] Antonio J. Jara, R.M. Silva, Jorge Sa Silva, Miguel A. Zamora, and Antonio F. Skarmeta, "Mobile ip-based protocol for wireless personal area networks in critical environments", *Wireless Personal Communications*, vol. 61, no. 4, pp. 711–737, 2011, doi:10.1007/s11277-011-0428-y.

[37] Antonio J Jara, Miguel A Zamora, and Antonio FG Skarmeta, "An architecture based on internet of things to support mobility and security in medical environments", in *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*. IEEE, 2010, pp. pp. 1–5.

[38] Antonio J Jara, Miguel A Zamora, and Antonio FG Skarmeta, "Intra-mobility for hospital wireless sensor networks based on 6lowpan", in *Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on*. IEEE, 2010, pp. pp. 389–394.

[39] Adam Dunkels, "uip-a free small tcp/ip stack", 2002, `http://www.sics.se/adam/uip`.

[40] Jonathan Hui and Pascal Thubert, "Rfc 6282: Compression format for ipv6 datagrams over ieee 802.15.4-based networks", *IETF*, 2011.

[41] Miguel Castro, Antonio J Jara, and Antonio Skarmeta, "Architecture for improving terrestrial logistics based on the web of things", *Sensors*, vol. 12, no. 5, pp. pp. 6538–6575, 2012.

[42] Nhon Chu, Djelal Raouf, Bruno Corlay, Mohamed Ammari, Nenad Gligoric, Srdjan Krco, Nemanja Ognjanovic, and Aleksandar Obradovic, "Oma dm v1. x compliant lightweight device management for constrained m2m devices", 2013, `http://openmobilealliance.org/about-oma/work-program/m2m-enablers/`.

[43] Z Shelby and C Chauvenet, "The ipso application framework. draft draft-ipso-app-framework-04", 2012, `http://www.ipso-alliance.org/wp-content/media/draft-ipso-app-framework-04.pdf`.

[44] Antonio J Jara, Francisco J Blaya, Miguel A Zamora, and A Skarmeta, "An ontology and rule based intelligent information system to detect and predict myocardial diseases", in *Information Technology and Applications in Biomedicine, 2009. ITAB 2009. 9th International Conference on*. IEEE, 2009, pp. pp. 1–6.

[45] R. Carroll, R. Cnossen, M. Schnell, and D. Simons, "Continua: An interoperable personal healthcare ecosystem", *IEEE Pervasive Computing*, vol. 6, no. 4, pp. pp. 90–94, 2007, doi:10.1109/MPRV.2007.72.

[46] Antonio J. Jara, Madeleine Rosas-Valera, Miguel Angel Zamora, and Antonio F. Skarmeta, "Improving treatment compliance and identification of adverse drug event among tb patients through use of hand-held personal device", in *Third International Conference on Improving Use of Medicines (ICIUM 2011)*, 2011, Antalya, Turkey.

[47] Miguel Angel Zamora, Antonio F. Skarmeta, Antonio J. Jara, Jose Lopez, and Alfredo Quesada, "System, device and method for detection of encapsulated objects (sistema, dispositivo y método para la detección de objetos encapsulado)", 2012, Application no: P-201230267-SE, Being exploited by: Flowlab S.L.

[48] José Santa, Miguel A Zamora-Izquierdo, Antonio J Jara, and Antonio F Gómez-Skarmeta, "Telematic platform for integral management of agricultural/perishable goods in terrestrial logistics", *Computers and Electronics in Agriculture*, vol. 80, pp. pp. 31–40, 2012.

[49] Antonio J Jara, Maria Concepcion Parra, and Antonio F Skarmeta, "Participative marketing: Extending social media marketing through the identication and interaction capabilities from the internet of things", *Personal and Ubiquitous Computing*, 2013.

[50] Antonio J Jara, Pablo Lopez, David Fernandez, Jose F Castillo, Miguel A Zamora, and Antonio F Skarmeta, "Mobile digcovery: discovering and interacting with the world through the internet of things", *Personal and Ubiquitous Computing*, pp. pp. 1–16, 2013.

[51] Andrés L Bleda, Antonio J Jara, Rafael Maestre, Guadalupe Santa, and Antonio F Gómez Skarmeta, "Evaluation of the impact of furniture on communications performance for ubiquitous deployment of wireless sensor networks in smart homes", *Sensors*, vol. 12, no. 5, pp. pp. 6463–6496, 2012.

[52] GSC MSTF, "Preliminary list of global organizations, groups, assoications, fora, and other entities with a direct or indirect interest in m2m standardization", 2011, `http://www.gsc16.ca/english/documents/openplenary/GSC16-PLEN-42a1r1.xlsx`.

[53] Ernesto García Davis, Anna Calveras, and Ilker Demirkol, "Improving packet delivery performance of publish/subscribe protocols in wireless sensor networks", *Sensors*, vol. 13, no. 1, pp. pp. 648–680, 2013.

Appendix A

Impact Factors

I. IEEE Journal on Selected Areas in Communications

Figure A.1: Impact Factor of the IEEE Journal on Selected Areas in Communications based on the Journal Citation Report (JCR) Impact Factor of Thomson Reuters [1].

ISI Web of Knowledge℠

Journal Citation Reports®

WELCOME HELP RETURN TO JOURNAL

2011 JCR Science Edition

Rank in Category: IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS

Journal Ranking

For **2011**, the journal **IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS** has an Impact Factor of **3.413**.

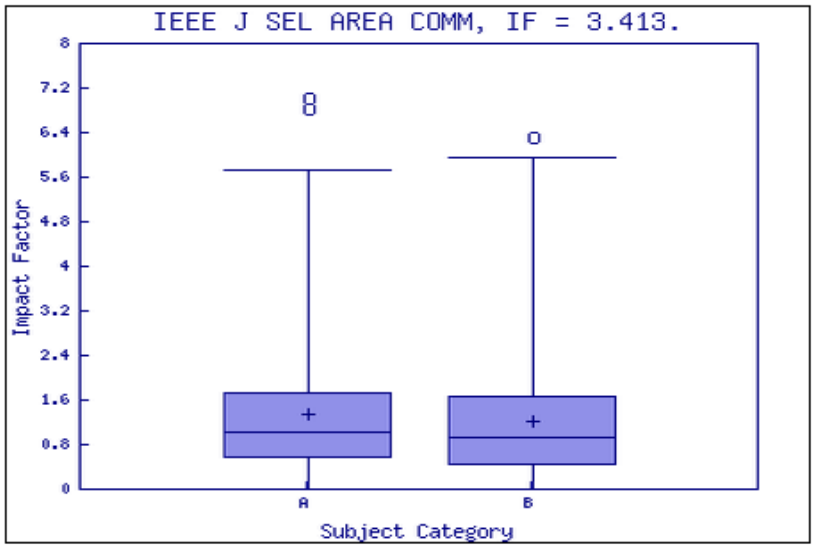
This table shows the ranking of this journal in its subject categories based on Impact Factor.

Category Name	Total Journals in Category	Journal Rank in Category	Quartile in Category
ENGINEERING, ELECTRICAL & ELECTRONIC	245	14	Q1
TELECOMMUNICATIONS	79	4	Q1

Category Box Plot

For **2011**, the journal **IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS** has an Impact Factor of **3.413**.

This is a box plot of the subject category or categories to which the journal has been assigned. It provides information about the distribution of journals based on Impact Factor values. It shows median, 25th and 75th percentiles, and the extreme values of the distribution.



Key

A - ENGINEERING, ELECTRICAL & ELECTRONIC

B - TELECOMMUNICATIONS

II. Mobile Information Systems

Figure A.2: Impact Factor of the Journal of Mobile Information Systems based on the Journal Citation Report (JCR) Impact Factor of Thomson Reuters [1].

ISI Web of Knowledge℠

Journal Citation Reports®

WELCOME HELP RETURN TO JOURNAL

2011 JCR Science Edition

Rank in Category: Mobile Information Systems

Journal Ranking

For **2011**, the journal **Mobile Information Systems** has an Impact Factor of **2.432**.

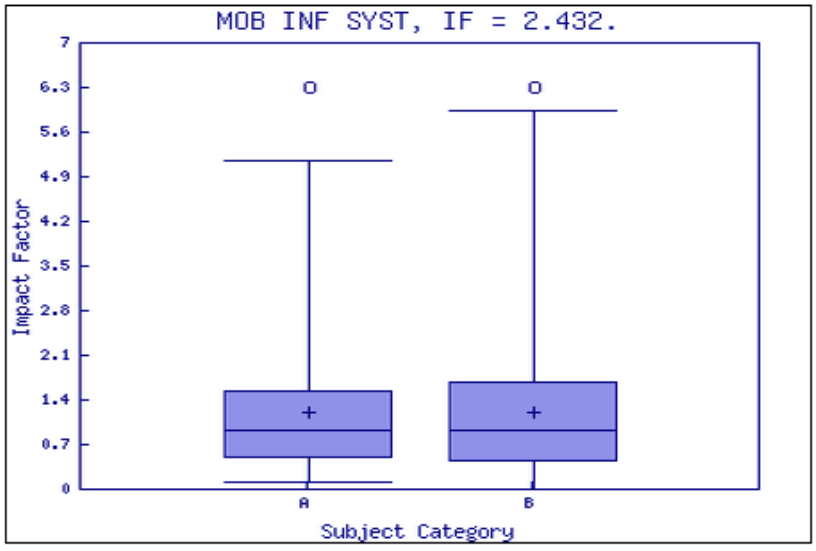
This table shows the ranking of this journal in its subject categories based on Impact Factor.

Category Name	Total Journals in Category	Journal Rank in Category	Quartile in Category
COMPUTER SCIENCE, INFORMATION SYSTEMS	135	11	Q1
TELECOMMUNICATIONS	79	8	Q1

Category Box Plot

For **2011**, the journal **Mobile Information Systems** has an Impact Factor of **2.432**.

This is a box plot of the subject category or categories to which the journal has been assigned. It provides information about the distribution of journals based on Impact Factor values. It shows median, 25th and 75th percentiles, and the extreme values of the distribution.



Key

A - COMPUTER SCIENCE, INFORMATION SYSTEMS

B - TELECOMMUNICATIONS

III. Sensors

Figure A.3: Impact Factor of the Journal of Sensors based on the Journal Citation Report (JCR) Impact Factor of Thomson Reuters [1].

ISI Web of Knowledge℠

Journal Citation Reports®

WELCOME HELP RETURN TO JOURNAL

2011 JCR Science Edition

Rank in Category: SENSORS

Journal Ranking

For **2011**, the journal **SENSORS** has an Impact Factor of **1.739**.

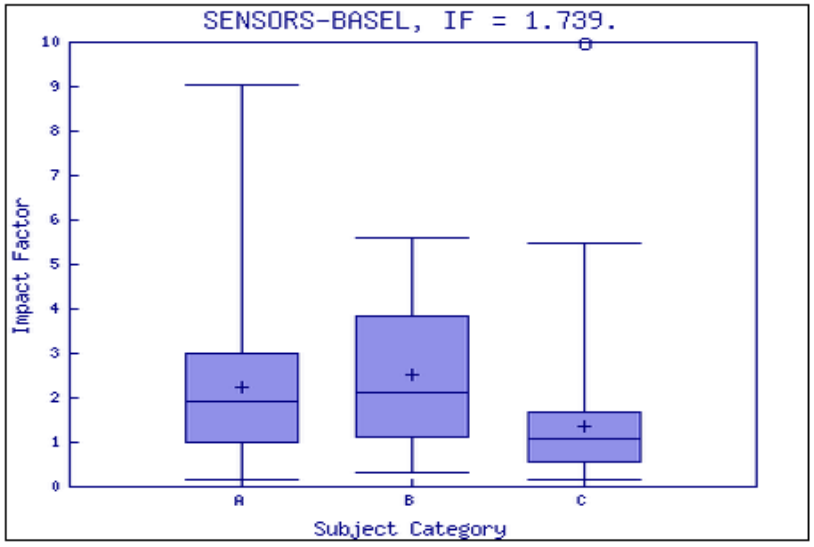
This table shows the ranking of this journal in its subject categories based on Impact Factor.

Category Name	Total Journals in Category	Journal Rank in Category	Quartile in Category
CHEMISTRY, ANALYTICAL	73	41	Q3
ELECTROCHEMISTRY	27	18	Q3
INSTRUMENTS & INSTRUMENTATION	58	14	Q1

Category Box Plot

For **2011**, the journal **SENSORS** has an Impact Factor of **1.739**.

This is a box plot of the subject category or categories to which the journal has been assigned. It provides information about the distribution of journals based on Impact Factor values. It shows median, 25th and 75th percentiles, and the extreme values of the distribution.



IV. Mathematical and Computer Modelling

Figure A.4: Impact Factor of the Journal of Mathematical and Computer Modelling based on the Journal Citation Report (JCR) Impact Factor of Thomson Reuters [1].

ISI Web of Knowledge℠

Journal Citation Reports®

WELCOME HELP RETURN TO JOURNAL

2011 JCR Science Edition

Rank in Category: MATHEMATICAL AND COMPUTER MODELLING

Journal Ranking

For **2011**, the journal **MATHEMATICAL AND COMPUTER MODELLING** has an Impact Factor of **1.346**.

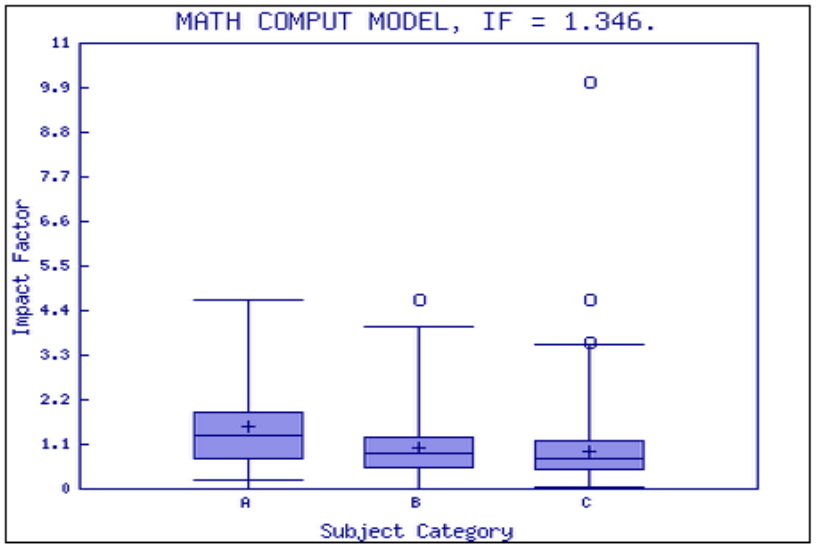
This table shows the ranking of this journal in its subject categories based on Impact Factor.

Category Name	Total Journals in Category	Journal Rank in Category	Quartile in Category
COMPUTER SCIENCE, INTERDISCIPLINARY APPLICATIONS	99	48	Q2
COMPUTER SCIENCE, SOFTWARE ENGINEERING	104	24	Q1
MATHEMATICS, APPLIED	245	40	Q1

Category Box Plot

For **2011**, the journal **MATHEMATICAL AND COMPUTER MODELLING** has an Impact Factor of **1.346**.

This is a box plot of the subject category or categories to which the journal has been assigned. It provides information about the distribution of journals based on Impact Factor values. It shows median, 25th and 75th percentiles, and the extreme values of the distribution.



V. Wireless Personal Communications

Figure A.5: Impact Factor of the Journal of Wireless Personal Communications based on the Journal Citation Report (JCR) Impact Factor of Thomson Reuters [1].

ISI Web of Knowledge℠

Journal Citation Reports®

WELCOME HELP RETURN TO JOURNAL

2011 JCR Science Edition

Rank in Category: WIRELESS PERSONAL COMMUNICATIONS

Journal Ranking

For **2011**, the journal **WIRELESS PERSONAL COMMUNICATIONS** has an Impact Factor of **0.458**.

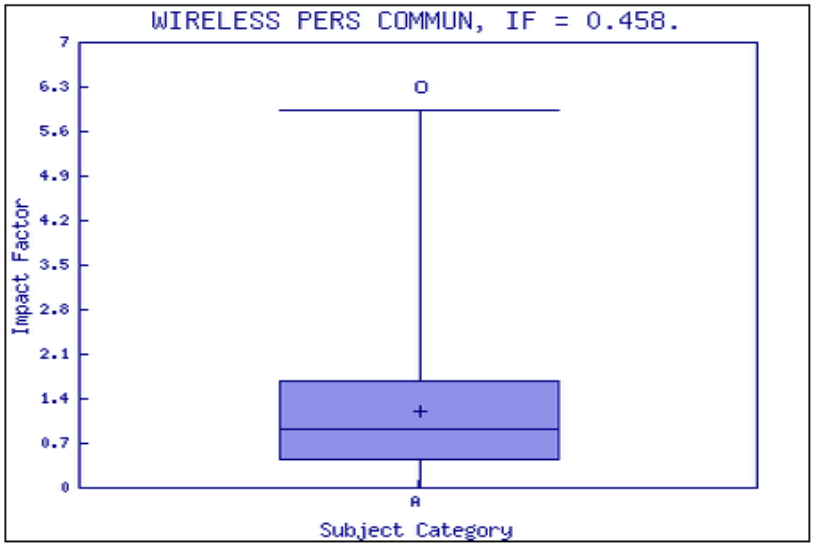
This table shows the ranking of this journal in its subject categories based on Impact Factor.

Category Name	Total Journals in Category	Journal Rank in Category	Quartile in Category
TELECOMMUNICATIONS	79	60	Q4

Category Box Plot

For **2011**, the journal **WIRELESS PERSONAL COMMUNICATIONS** has an Impact Factor of **0.458**.

This is a box plot of the subject category or categories to which the journal has been assigned. It provides information about the distribution of journals based on Impact Factor values. It shows median, 25th and 75th percentiles, and the extreme values of the distribution.



Key

A - TELECOMMUNICATIONS

VI. International Journal of Ad Hoc and Ubiquitous Computing

Figure A.6: Impact Factor of the International Journal of Ad Hoc and Ubiquitous Computing based on the Journal Citation Report (JCR) Impact Factor of Thomson Reuters [1].

ISI Web of Knowledge℠

Journal Citation Reports®

WELCOME HELP RETURN TO JOURNAL

2011 JCR Science Edition

Rank in Category: International Journal of Ad Hoc and Ubiquitous Com...

Journal Ranking

For **2011**, the journal **International Journal of Ad Hoc and Ubiquitous Com...** has an Impact Factor of **0.848**.

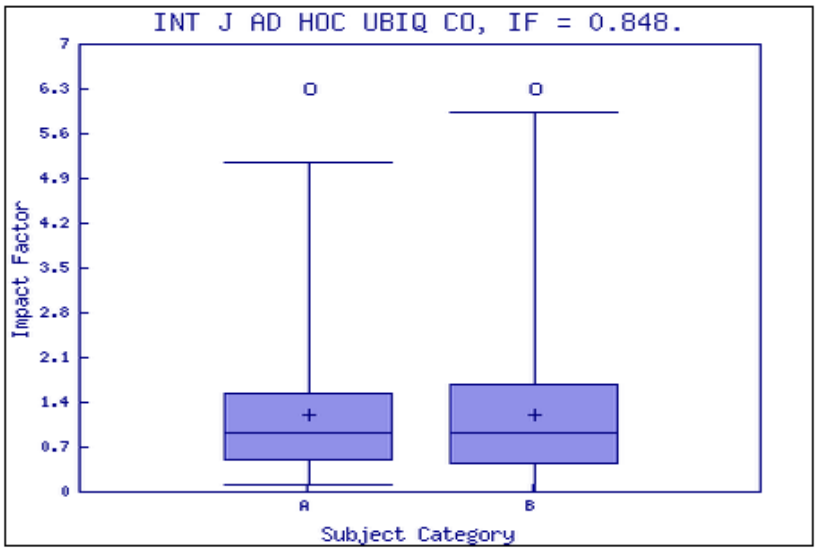
This table shows the ranking of this journal in its subject categories based on Impact Factor.

Category Name	Total Journals in Category	Journal Rank in Category	Quartile in Category
COMPUTER SCIENCE, INFORMATION SYSTEMS	135	80	Q3
TELECOMMUNICATIONS	79	47	Q3

Category Box Plot

For **2011**, the journal **International Journal of Ad Hoc and Ubiquitous Com...** has an Impact Factor of **0.848**.

This is a box plot of the subject category or categories to which the journal has been assigned. It provides information about the distribution of journals based on Impact Factor values. It shows median, 25th and 75th percentiles, and the extreme values of the distribution.



VII. Personal and Ubiquitous Computing

Figure A.7: Impact Factor of the Journal of Personal and Ubiquitous Computing based on the Journal Citation Report (JCR) Impact Factor of Thomson Reuters [1].

ISI Web of Knowledge℠

Journal Citation Reports®

WELCOME HELP RETURN TO JOURNAL

2011 JCR Science Edition

Rank in Category: Personal and Ubiquitous Computing

Journal Ranking

For **2011**, the journal **Personal and Ubiquitous Computing** has an Impact Factor of **0.938**.

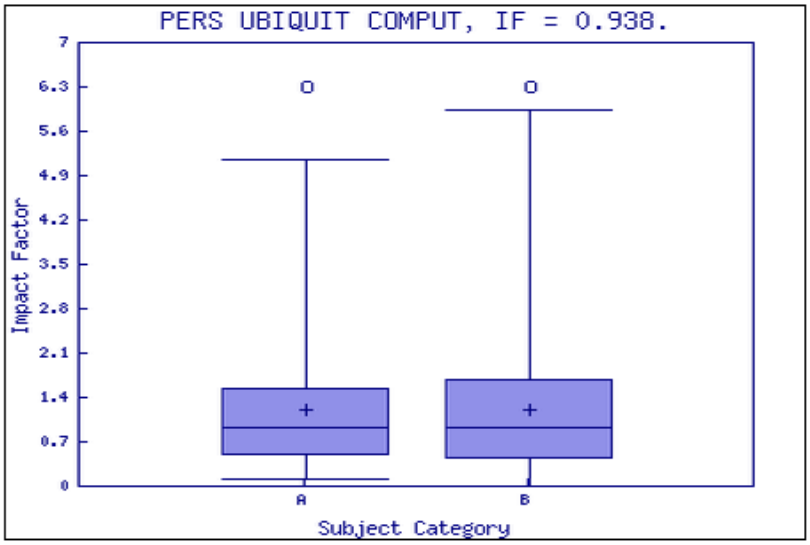
This table shows the ranking of this journal in its subject categories based on Impact Factor.

Category Name	Total Journals in Category	Journal Rank in Category	Quartile in Category
COMPUTER SCIENCE, INFORMATION SYSTEMS	135	67	Q2
TELECOMMUNICATIONS	79	40	Q3

Category Box Plot

For **2011**, the journal **Personal and Ubiquitous Computing** has an Impact Factor of **0.938**.

This is a box plot of the subject category or categories to which the journal has been assigned. It provides information about the distribution of journals based on Impact Factor values. It shows median, 25th and 75th percentiles, and the extreme values of the distribution.



Key

A - COMPUTER SCIENCE, INFORMATION SYSTEMS

B - TELECOMMUNICATIONS

VIII. Interacting with Computers

Figure A.8: Impact Factor of the Journal of Interacting with Computers based on the Journal Citation Report (JCR) Impact Factor of Thomson Reuters [1].

ISI Web of Knowledge℠

Journal Citation Reports®

WELCOME HELP RETURN TO JOURNAL

2011 JCR Science Edition

Rank in Category: INTERACTING WITH COMPUTERS

Journal Ranking

For **2011**, the journal **INTERACTING WITH COMPUTERS** has an Impact Factor of **1.233**.

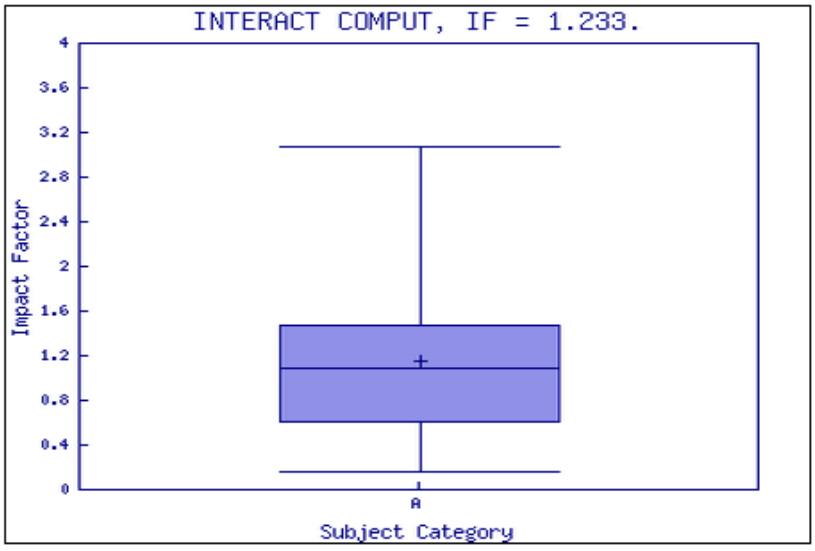
This table shows the ranking of this journal in its subject categories based on Impact Factor.

Category Name	Total Journals in Category	Journal Rank in Category	Quartile in Category
COMPUTER SCIENCE, CYBERNETICS	20	8	Q2

Category Box Plot

For **2011**, the journal **INTERACTING WITH COMPUTERS** has an Impact Factor of **1.233**.

This is a box plot of the subject category or categories to which the journal has been assigned. It provides information about the distribution of journals based on Impact Factor values. It shows median, 25th and 75th percentiles, and the extreme values of the distribution.



Key

A - COMPUTER SCIENCE, CYBERNETICS

IX. Journal of Universal Computer Science

Figure A.9: Impact Factor of the Journal of Universal Computer Science based on the Journal Citation Report (JCR) Impact Factor of Thomson Reuters [1].

ISI Web of Knowledge℠

Journal Citation Reports®

WELCOME HELP RETURN TO JOURNAL

2011 JCR Science Edition

Rank in Category: JOURNAL OF UNIVERSAL COMPUTER SCIENCE

Journal Ranking

For **2011**, the journal **JOURNAL OF UNIVERSAL COMPUTER SCIENCE** has an Impact Factor of **0.398**.

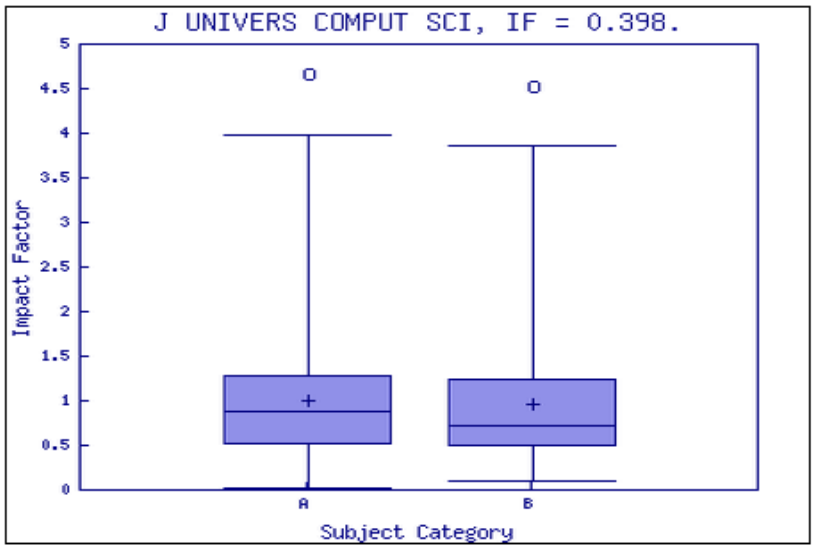
This table shows the ranking of this journal in its subject categories based on Impact Factor.

Category Name	Total Journals in Category	Journal Rank in Category	Quartile in Category
COMPUTER SCIENCE, SOFTWARE ENGINEERING	104	85	Q4
COMPUTER SCIENCE, THEORY & METHODS	99	84	Q4

Category Box Plot

For **2011**, the journal **JOURNAL OF UNIVERSAL COMPUTER SCIENCE** has an Impact Factor of **0.398**.

This is a box plot of the subject category or categories to which the journal has been assigned. It provides information about the distribution of journals based on Impact Factor values. It shows median, 25th and 75th percentiles, and the extreme values of the distribution.



Key

A - COMPUTER SCIENCE, SOFTWARE ENGINEERING

B - COMPUTER SCIENCE, THEORY & METHODS

Appendix B

Extra Journal paper: An internet of things-based personal device for diabetes therapy management in Ambient Assisted Living (AAL)

Title:	An internet of things - based personal device for diabetes therapy management in ambient assisted living (AAL)
Authors:	Antonio J. Jara, Miguel A. Zamora, Antonio F. Skarmeta
Journal:	Personal and Ubiquitous Computing
ISSN:	Print (1617-4909) Online (1617-4917)
Impact factor:	0,938 (2011) - Position 67 out of 135 (See section VII)
Publisher:	Springer-Verlag
Volume:	15
Number:	4
Pages:	431-440
Year:	2011
Month:	April
DOI:	10.1007/s00779-010-0353-1
Link:	http://link.springer.com/article/10.1007/s00779-010-0353-1
State:	Published

This journal paper is out of the compendium, because it was published before the PhD proposal. This has been considered to include it as an appendix, since this presents a relevant use case of the proposed communication architecture for the diabetes therapy.