UNIVERSITAT POLITÈCNICA DE VALÈNCIA
DEPARTAMENTO DE COMUNICACIONES

DISEÑO, ESPECIFICACIÓN, IMPLEMENTACIÓN Y VALIDACIÓN DE HABILITADORES DIGITALES PARA LA INTEROPERABILIDAD DE PLATAFORMAS DE INTERNET DE LAS COSAS (IoT)

TESIS DOCTORAL

Régel González Usach

Director:
Carlos Enrique Palau Salvador

Valencia, España
Septiembre 2021

Parte de esta tesis doctoral ha sido realizada dentro del grupo de investigación SATRD (Sistemas y Aplicaciones de Tiempo Real Distribuido) como parte de las actividades del proyecto de Investigación INTER-IoT financiado por la Comisión Europea dentro del Programa Marco de Investigación e Innovación Horizonte 2020 dentro del acuerdo de subvención nº 687283, como parte de las actividades del proyecto SAFE-ECH financiado por el Ministerio de Industria, Economía y Competitividad (MINECO) bajo el acuerdo de subvención RTC2015-4502-1, y como parte de las actividades del proyecto ACTIVAGE financiado por la Comisión Europea dentro del programa Marco de Investigación e Innovación Horizonte 2020 bajo el acuerdo de subvención nº 732679.

Agradecimientos

A todas las personas que han hecho que esta tesis sea posible desde la universidad y desde los proyectos de investigación en que he participado.

A mis amigos y personas cercanas, los cuales me han animado siempre durante el periodo de desarrollo de la tesis y me han ayudado de distintas maneras a lo largo del proceso de escritura de este documento.

Resumen

Internet de las Cosas (IoT) es un paradigma tecnológico que está transformando y revolucionando el mundo en el cual vivimos, liderando la transformación digital y generando enormes posibilidades desde el punto de vista tecnológico que pueden solucionar grandes problemas y retos en nuestra sociedad y efectuar cambios profundos en nuestra economía e industria, y transformar nuestra vida cotidiana . Sin embargo, para poder obtener estos grandes beneficios y explotar todo su potencial todavía hace falta abordar y resolver grandes retos tecnológicos asociados. La interoperabilidad es el mayor reto tecnológico del paradigma IoT, conjuntamente con la seguridad, a causa de la vasta heterogeneidad inherente del universo IoT a todos los niveles y la falta de una estandarización global aceptada de facto capaz de alinear sus diferentes elementos y aspectos, que actualmente no se considera viable conseguir.

La capacidad de elementos y sistemas de comunicarse y compartir información de manera efectiva entre ellos habilita intercambios de información relevante, coordinación o cooperación entre sí y sinergias. La fragmentación de la información de sistemas IoT y falta inherente de interoperabilidad en este paradigma causa graves problemas económicos y tecnológicos, e impide las sinergias entre sistemas. Se considera que la carencia de interoperabilidad es el mayor obstáculo para la formación de un ecosistema global de IoT, un hito en la transformación digital, puesto que impide la integración horizontal de mercados verticales y deja una gran fragmentación entre los sistemas basados en información obtenida con la tecnología IoT.

IoT, uno de los paradigmas o habilitadores clave de la transformación digital, está enormemente limitada por carencias de interoperabilidad, que impiden su crecimiento, evolución y despliegue de todo su potencial. Es absolutamente crítico resolver el problema de falta intrínseca de interoperabilidad entre plataformas IoT para poder avanzar tecnológicamente hacia el Internet del Futuro, la Nueva Generación de IoT y la digitalización del mundo.

La habilitación de la interoperabilidad entre sistemas y a lo largo de los sistemas, para conseguir un ecosistema interconexionado global, es un reto complejo y de múltiples facetas. Entre ellas, la interoperabilidad semántica, que implica el entendimiento completo, automático y sin ambigüedades de la información compartida entre sistemas, es singularmente compleja de obtener entre plataformas IoT a causa de la alta heterogeneidad entre sus modelos de información.

En esta tesis se abarca el estudio, diseño, especificación, implementación y validación de habilitadores digitales (herramientas tecnológicas que promueven la digitalización del mundo) para establecer interoperabilidad en IoT en diferentes niveles (técnico, sintáctico, semántico) con especial enfoque en la interoperabilidad semántica entre plataformas heterogéneas, uno de los retos técnicos más complejos actualmente en IoT. También se abordan en el estudio y construcción de estos habilitadores temas a resolver de Internet del Futuro y la Nueva Generación de Internet de las Cosas.

Resum

Internet de les Coses (IoT) és un paradigma tecnològic que està transformant i revolucionant el món en el qual vivim, liderant la transformació digital i generant enormes possibilitats des del punt de vista tecnològic que poden solucionar grans problemes i reptes en la nostra societat i efectuar canvis profunds en la nostra economia i indústria, i transformar la nostra vida quotidiana. No obstant això, per a poder obtindre aquests grans beneficis i explotar tot el seu potencial encara fa falta abordar i resoldre grans reptes tecnològics associats. La interoperabilitat és el major repte tecnològic del paradigma IoT, conjuntament amb la seguretat, a causa de la vasta heterogeneïtat inherent de l'univers IoT a tots els nivells i la falta d'una estandardització global acceptada de facto capaç d'alinear els seus diferents elements i aspectes, que actualment no es considera viable aconseguir.

La capacitat d'elements i sistemes de comunicar-se i compartir informació de manera efectiva entre ells habilita intercanvis d'informació rellevant, coordinació o cooperació entre si i sinergies. La fragmentació de la informació de sistemes IoT i falta inherent d'interoperabilitat en aquest paradigma causa greus problemes econòmics i tecnològics, i impedeix les sinergies entre sistemes. Es considera que la manca d'interoperabilitat és el major obstacle per a la formació d'un ecosistema global de IoT, una fita en la transformació digital, ja que impedeix la integració horitzontal de mercats verticals i deixa una gran fragmentació entre els sistemes basats en informació obtinguda amb la tecnologia IoT.

La IoT, un dels paradigmes o habilitadors clau de la transformació digital, està enormement limitada per manques d'interoperabilitat, que impedeixen el seu creixement, evolució i desplegament de tot el seu potencial. És absolutament crític resoldre el problema de falta intrínseca d'interoperabilitat entre plataformes IoT per a poder avançar tecnològicament cap a la Internet del Futur, la Nova Generació de IoT i la digitalització del món.

L'habilitació de la interoperabilitat entre sistemes i al llarg dels sistemes, per a aconseguir un ecosistema interconnectat global, és un repte complex i de múltiples facetes. Entre elles, la interoperabilitat semàntica, que implica l'enteniment complet, automàtic i sense ambigüitats de la informació compartida entre sistemes, és singularment complexa d'obtindre entre plataformes IoT a causa de l'alta heterogeneïtat entre els seus models d'informació.

En aquesta tesi s'abasta l'estudi, disseny, especificació, implementació i validació d'habilitadors digitals (eines tecnològiques que promouen la digitalització del món) per a establir interoperabilitat en IoT en diferents nivells (tècnic, sintàctic, semàntic) amb especial enfocament en la interoperabilitat semàntica entre plataformes heterogènies, un dels reptes tècnics més complexos actualment en IoT. També s'aborden en l'estudi i construcció d'aquests habilitadors temes a resoldre d'Internet del Futur i la Nova Generació d'Internet de les Coses.

Abstract

The Internet of Things (IoT) is a technological paradigm that is transforming and revolutionising the world we live in, leading the digital transformation and generating enormous technological possibilities that could solve major challenges in our society, effect profound changes in our economy and industry and transform our daily lives. However, in order to realise these great benefits and exploit IoT's full potential, there are major associated technological challenges to be addressed and solved. Interoperability is the biggest technological challenge of the IoT paradigm, together with security, because of the vast inherent heterogeneity in IoT at all levels and the lack of a de facto global standard capable of aligning its different elements and aspects, which is currently not considered feasible to achieve.

The ability of elements and systems to communicate and share information effectively with each other enables exchanges of relevant information, coordination or cooperation with each other and synergies. The fragmentation of information in IoT systems and inherent lack of interoperability in this paradigm causes serious economic and technological problems, and prevents synergies between systems. The lack of interoperability is considered to be the biggest obstacle to the formation of a global IoT ecosystem, a milestone in the digital transformation, as it prevents horizontal integration of vertical markets and leaves a large fragmentation between systems based on IoT-derived information.

IoT, one of the key paradigms or enablers of digital transformation, is severely constrained by interoperability gaps, which impede its growth, evolution and deployment of its full potential. It is absolutely critical to solve the problem of intrinsic lack of interoperability between IoT platforms in order to move technologically towards the Future Internet, the Next Generation IoT and the digitisation of the world.

The enablement of interoperability between and across systems to achieve a globally interconnected ecosystem is a complex and multi-faceted challenge. Among them, semantic interoperability, which implies an automatic unambiguous understanding of the information shared between systems, is hardly feasible between IoT platforms due to the high heterogeneity of information models.

This thesis covers the study, design, specification, implementation and validation of digital enablers to establish IoT interoperability at different levels (technical, syntactic, semantic) with special focus on semantic interoperability between heterogeneous platforms, one of the most complex technical challenges currently in IoT. The study and construction of these enablers also address issues to solve in the Future Internet and the Next Generation of the Internet of Things.

Índice de contenidos

Capítulo 1
Introducción

"La mente que se abre a una nueva idea jamás vuelve a su tamaño original"

Albert Einstein

1.1. Motivación

Internet de las Cosas (IoT) [1] es un reciente paradigma tecnológico que está transformando y revolucionando el mundo en el que vivimos. A pesar de que tan solo hemos empezado a vivir una fase inicial y meramente arañado su potencial son innegables los cambios profundos que ha provocado en nuestra sociedad, industria y economía y que podemos notar en nuestra vida cotidiana. Internet de las Cosas constituye un paradigma que podría solucionar graves problemas en nuestra sociedad actualmente, tales como la asistencia a enfermos [2] (siendo remota, automática y disponible en cualquier momento), en épocas de pandemia y confinamiento podría evitar el aislamiento social de las personas más vulnerables y desprotegidas, habilitar monitorización de personas, digitalización de nuestro mundo, optimización de la

industria hacia la Industria 4.0 [3], creación de gemelos digitales [4] y un habilitador de la herramienta que podría lanzar a Europa a ser líder digital. Sin embargo, para poder obtener estos grandes beneficios y explotar todo su potencial aún hace falta abordar y resolver grandes retos tecnológicos asociados.

La interoperabilidad es uno de los mayores retos tecnológico en el universo IoT debido a la gran heterogeneidad intrínseca de la Internet de las Cosas, que comprende una miríada de estándares, tecnologías de comunicación, protocolos, modelos de representación de la información y formatos de datos dispares, no alineados por ningún estándar global de facto [5].

Esta fragmentación de la información de la IoT y falta intrínseca de interoperabilidad causa graves problemas económicos y tecnológicos, e impide las sinergias entre sistemas [6]. Se ha llegado a estimar que más del 40% de los beneficios potenciales de IoT no son posibles sin mayor interoperabilidad [7]. La visión del futuro de la IoT, la cual prevé un mundo completamente interconectado en que las personas interactuarán de manera natural con interfaces integradas en los entornos diarios, muy lejanas de las interfaces técnicas actuales, tiene como requisito crucial la habilitación de interoperabilidad sin barreras entre los distintos sistemas, plataformas y elementos IoT.

Esta falta de interoperabilidad, es especialmente difícil de solucionar en el caso de interoperabilidad de plataformas IoT, que gestionan torrentes de datos masivos IoT en tiempo real procedentes de dispositivos inteligentes o cosas, y tienen modelos semánticos de información y formatos de datos dispares, además de usar estándares, protocolos e interfaces heterogéneos. Esto es así ya que cada plataforma emplea diferentes formatos de datos y modelos semánticos de información, creando silos verticales de información aislados entre ellos y el resto de la IoT [8].

Además, hay que tener en cuenta que la interoperabilidad de los sistemas de información tiene muchos grados y niveles, siendo el nivel semántico el más elevado, el cual permite que los distintos sistemas y plataformas heterógeneos que componen la IoT puedan entender el significado de la información que reciben de otros sistemas, pudiendo compartir información entre ellos sin barreras y ser capaces de utilizarla inteligente y efectivamente [9]. Este tipo de interoperabilidad implica la consecución de otros niveles previos (sintáctico y técnico), así que para poder obtener sus

beneficios es necesario habilitar todos ellos. Así mismo estos niveles tienen que estar habilitados transversalmente a lo largo de todas las capas que componen un sistema IoT, las cuales tienen necesidades muy distintas y específicas que no deben ser ignoradas. Por todo ello, la habilitación de la interoperabilidad entre sistemas y a lo largo de los sistemas, para conseguir un ecosistema interconectado global, es un reto especialmente complejo y de múltiples facetas [6].

Esta tesis aborda el estudio, diseño y utilización de habilitadores digitales específicos para permitir la interoperabilidad en sistemas y plataformas IoT heterogéneos (los cuales emplean distintos modelos de información, semántica, formato de datos e interfaces de comunicación). Esta interoperabilidad se aborda en diferentes niveles (técnica, sintáctica y semántica), teniendo especial atención el grado más alto de interoperabilidad entre sistemas: la interoperabilidad semántica. Este tipo de interoperabilidad implica el entendimiento completo de manera automática del significado de la información compartida entre sistemas, y su consecución entraña generalmente gran complejidad. En algunos casos estos habilitadores abordan paradigmas de la Internet Futura [10]-en la cual se desplegará la evolución del Internet de las Cosas-, y grandes pilares tecnológicos de la transformación digital como la computación en la nube y la inteligencia artificial.

1.2. Habilitadores digitales

Los habilitadores digitales son las distintas herramientas tecnológicas que tienen la capacidad de habilitar o permitir la transformación digital de nuestro mundo. Un ejemplo de ellas son, entre otras, el uso de Internet de las Cosas [11], Big Data [12] y la Computación en la Nube [13].

Estas tecnologías tienen un papel clave en la digitalización de la industria, transformándola hacia el nuevo paradigma de la Industria 4.0 [3]. No obstante, estos habilitadores digitales no solo están presentes en la digitalización de la industria, proceso por el que son popularmente conocidos, sino que pueden adoptar otros roles o papeles clave importantes en la digitalización del mundo actual, como por ejemplo ayudar a la habilitación de la interoperabilidad en el heterogéneo mundo de IoT.

En esta tesis se investiga el difícil reto que constituye la interoperabilidad en IoT, y se trata del uso de diversas herramientas tecnológicas (habilitadores digitales) para conseguir habilitar interoperabilidad entre distintos sistemas y plataformas IoT.

1.3. Principales contribuciones

Se presentan a continuación en las siguientes secciones las publicaciones generadas en el marco de la tesis doctoral. Estas están clasificadas como artículos en revistas, libros, capítulos de libro y artículos en congresos internacionales.

1.3.1. Artículos en revistas

- D. Sarabia-Jácome, **R. Gonzalez-Usach**, C. Palau, M. Esteve (2020) Highly-Efficient Fog-Based Deep Learning AAL Fall Detection System. *En Internet of Things Journal Vol 11*
- C. Valero, A. Medrano, **R. Gonzalez-Usach**, M. Julian, Giuseppe Fico et al. (2021) AIoTES: Setting the principles for semantic interoperable and modern IoT-enabled reference architecture for Active and Healthy Ageing ecosystem. En *Computer Communications*
- E. Ordonez-Jimenez, H. Gil, R. Oltra, **R. Gonzalez-Usach** (2015) Information Technology Skills (e-skills) importance in Productive Sectors. Research Proposal in the Transport Sector of the Valencian Community. *En 3C TIC (Edición núm. 12) Vol.4 – Nº 1*

1.3.2. Libros

- A. Bröring, A. Zappa, O. Vermesan, K. Främling, A. Zaslavsky, **R. Gonzalez-Usach** et al., (2018) Advancing IoT Platforms Interoperability. *Publicado por River Publishers*

1.3.3. Capítulos de libro

- **R. Gonzalez-Usach,** M. Kuehlewind (2012) Implementation and Evaluation of Coupled Congestion Control for Multipath TCP. En *Information and Communications Technologies* (EUNICE 2012). (173 - 182). Springer. Lecture Notes in Computer Science.
- **R. Gonzalez-Usach,** D. Yacchirema, V. Collado, M. Esteve, C. Palau (2017) AmI Open Source System for the Intelligent Control of Residences for the Elderly. En: *Interoperability, Safety and Security in IoT*, pp. 46–52. Springer.
- **R. Gonzalez-Usach,** C. E. Palau, M. Julian, A. Belsa, A., M. Llorente et al. (2018) IoT Interoperability: Use Cases, Applications and Implementation Aspects. En: IERC Book 2018- Distributed Intelligence at the Edge and Human Machine-To-Machine Cooperation, pp.139-173. River Publishers.
- A. Bröring, A. Zappa, O. Vermesan, K. Främling, A. Zaslavsky, **R. Gonzalez-Usach** et al., (2018) IoT platforms landscape*. En: Advancing IoT Platforms Interoperability. Publicado por River Publishers*
- A. Bröring, A. Zappa, O. Vermesan, K. Främling, A. Zaslavsky, **R. Gonzalez-Usach** et al., (2018) IoT Platforms interoperability concepts, approaches and principles *En: Advancing IoT Platforms Interoperability. Publicado por River Publishers*
- A. Bröring, A. Zappa, O. Vermesan, K. Främling, A. Zaslavsky, **R. Gonzalez-Usach** et al., (2018) IoT-EPI Projects approaches addressing IoT platforms interoperability *En: Advancing IoT Platforms Interoperability. Publicado por River Publishers*
- **R. Gonzalez-Usach,** D. Yacchirema, M. Julian, C. Palau (2019) Interoperability in IoT. En: *Handbook of Research on Big Data and the IoT*, pp. 149–173. IGI Global.
- D. Sarabia, **R. Gonzalez-Usach**, C. Palau (2019) IoT Big Data Architectures, Approaches, and Challenges: A Fog-Cloud Approach

. En: *Handbook of Research on Big Data and the IoT*, pp. 149–173. IGI Global.

- **R. Gonzalez-Usach**, M Julian, M. Esteve, C. Palau (2021) IoT Semantic Interoperability applied to Active and Health Ageing. *En Semantic Internet of Things.* Springer
- **R. Gonzalez-Usach**, C. Palau, M. Llorente (2021) IoT Platform Ecosystem Building. En *Internet of Things,* Springer (Aceptado)
- P. Jimenez, **R. Gonzalez-Usach**, M. Llop, C. Palau (2021) Requirements for Interoperability, *En Internet of Things,* Springer (Aceptado)
- D. Sarabia, **R. Gonzalez-Usach**, C. Palau (2021) IoT Big Data Architectures, Approaches, and Challenges: A Fog-Cloud Approach. En: *Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing* (227 - 250). IGI Global

1.3.4. Artículos en congresos internacionales

- **R. Gonzalez-Usach**, M. Kuhlewind (2012) Implementation and Evaluation of Coupled Congestion Control for Multipath TCP. En la conferencia 18 EUNICE Conference en *Tecnologías de la Información y Comunicación*, Budapest, Hungria
- M. Kuhlewind, **R. Gonzalez-Usach** (2012) A Delay-based approach for MPTCP Congestion Control, en la conferencia **IETF 84,** Vancouver (Canadá)
- **R. Gonzalez-Usach**, J. Pradilla, M. Esteve, C. E. Palau (2016) Hybrid Delay-based Congestion Control for Multipath TCP en la conferencia IEEE MELECON 2016
- J. Pradilla, **R. Gonzalez-Usach**, C.E. Palau, M. Esteve,SOS-CoAP Proxy Design. En la conferencia IEEE MELECON 2016

- **R. Gonzalez-Usach**, V. Collado, M. Esteve y C. Palau (2017) AAL open source system for the monitoring and intelligent control of nursing homes en la conferencia IEEE ICNSC 2017
- **R. Gonzalez-Usach,** D. Yacchirema, V. Collado, C. Palau, *et al.* (2017) AmI Open Source System for the Intelligent Control of Residences for the Elderly. En la *conferencia InterIoT 2017*
- D. Yacchirema, **R. Gonzalez-Usach**, C**.** Palau, C., et al. (2018) Interoperability of IoT Platforms applied to the transport and logistics domain. En la *conferencia Transport Research Arena 2018*. Publicación en abierto: Zenodo. doi:10.5281/zenodo.1451428
- **R. Gonzalez-Usach**, D. Sarabia, C. Palau, M. Esteve (2018) Interoperable IoT Dynamic Lighting for Port Terminal Containers. En la conferencia TRA 2018
- **R. Gonzalez-Usach**, M. Julian, C. Palau, M. Esteve (2021) Federation of AAL& AHA systems through semantically interoperable framework. .En *la conferencia IEEE ICC 2021*
- D. Lioprasitis, A. Priovolos, G. Gardikis, S. Pantazis, S. Costicoglou, A. Perentos, E. Hadjioannou, M. Georgiades, A. Phinikarides, A. Fornes, R. Gonzalez-Usach, C. Palau, M. Esteve (2021) Satellite edge computing for 5G rural applications. En la *conferencia IEEE MeditCom 2021.*

1.3.5. Participación en proyectos de investigación

- Proyecto INTER-IoT: ***"Interoperability of Heterogeneous IoT Platforms***" financiado por la Comisión Europea dentro del Programa Horizonte 2020 bajo el acuerdo de subvención nº 687283, con el objetivo de obtener soluciones de interoperabilidad en IoT, y coordinado por la UPV. Con duración desde Enero de 2016 a Diciembre de 2018.

- Proyecto ACTIVAGE: **"Activating Innovative IoT Smart Living Environments for Ageing Well"** orientado a entornos inteligentes para la mejora de la calidad de vida de la tercera edad, permitiendo una vida más activa, segura e independiente gracias al uso de hogares inteligentes especialmente diseñados para la población de mayor edad y el uso de dispositivos IoT. Financiado por la Comisión Europea dentro del Programa Horizonte 2020 con el acuerdo de subvención nº 732679. Con duración desde Enero de 2017 a Junio de 2020.
- Proyecto SAFE-ECH: "**Sistema de Monitorización y Control Seguro de Residencias de la Tercera Edad**" para la creación de un sistema inteligente de código abierto para la monitorización de residencias, permitiendo la creación de entornos inteligentes para la mejora de la calidad de vida de la tercera edad en residencias. Con duración desde Enero de 2015 a Diciembre de 2017.
- Proyecto 5GENESIS: **"*5th Generation End-to-end Network, Experimentation, System Integration, and Showcasing*"**, orientado a la creación de un marco de experimentación para el desarrollo 5G. Financiado por la Comisión Europea dentro del Programa Horizonte 2020 con el acuerdo de subvención nº 815178. Con duración desde Julio de 2018 a Diciembre de 2021.
- Proyecto EVOLVED-5G: **"*Experimentation and Validation Openness for Longterm evolution of VErtical inDustries in 5G era and beyond*"** dedicado a la creación de un marco abierto de experimentación y validación de aplicaciones de red 5G para la explotación de las ventajas de la funcionalidad de esta nueva generación de redes móbiles. Esta explotación de 5G se hará sobre casos de aplicación de IoT en Industria 4.0, que serán desarrollados y validados en el proyecto. Financiado por la Comisión Europea dentro del Programa Horizonte 2020 con el acuerdo de subvención nº 101016608. Con duración desde Enero de 2021 a la actualidad.

1.3.6. Estancias

Estancia en el centro de investigación SIMULA Research Laboratory (Oslo, 2016) – Investigación de comportamientos de tipos de traffico Multipath TCP según su tipo de aplicación en puntos de red compartidos. Simulaciones y escenarios programados con el emulador *CORE emulator*.

1.3.7. Software

- Módulo de control de congestión TCP y MPTCP dentro del kernel de Linux para el sistema operativo Linux.
- Sistema central SAFE-ECH para la gestión inteligente de residencias mediante el uso de tecnología IoT.
- Módulo externo al traductor semántico IPSM para regular el flujo externo de datos a la velocidad de traducción mediante el uso de técnicas de presión inversa.
- Módulos del framework AIoTES (independientes o como parte del framework):
  - SIL TOOL (suscriptor asistido a información IoT de dispositivos y plataformas gestionada por la SIL).
  - AIOTES IDE (IDE conteniendo cuatro herramientas de desarrollo diferentes: ServiceComposer, ClickDigital, CodeTemplates, CodeGenerator).
  - Virtualización de las herramientas utilizando Docker y Docker Compose.
  - Integración de seguridad OATH 2.0, que implica cambios en el enrutado, flujo del código y llamadas a backend.
- Scripts para la gestión de la seguridad OATH 2.0 dentro del framework AIOTES.

- Alineamientos semánticos para habilitar la traducción semántica entre múltiples plataformas.
- Demostradores del uso de la SIL
- Contribución a la integración del framework AIoTES.
- Colaboración con la actualización, testeo, soporte y documentación de puentes de comunicación del componente Inter-MW.
- Colaboración con las clases de mensajería de Inter-MW.

1.4. Objetivos

Esta tesis se enfoca en el problema de la interoperabilidad en IoT y la búsqueda y estudio de soluciones, y en especial en sus dos mayores desafíos:

- el crecimiento exponencial del tráfico en Internet, con la consiguiente sobrecarga de redes y limitaciones a su capacidad de proporcionar interoperabilidad técnica o capacidad de establecer la comunicación a través de ellas
- la interoperabilidad semántica entre plataformas y sistemas IoT

La investigación desarrollada en el marco de esta tesis tiene la siguiente meta:

Definir, diseñar e implementar soluciones de interoperabilidad basadas en habilitadores digitales o herramientas tecnológicas que permitan la comunicación sin fisuras entre o sobre plataformas y sistemas IoT heterogéneos.

Con el fin de conseguir esta meta principal, se han definido los siguientes objetivos:

O1. Identificación de la situación actual de la interoperabilidad en IoT, enmarcando el problema de la interoperabilidad en el paradigma de IoT con especial atención sobre la interoperabilidad semántica entre plataformas.

Identificación de los niveles de interoperabilidad, identificación de las necesidades específicas en cada capa o punto específico de los sistemas IoT e identificación de las causas y consecuencias de la falta intrínseca de interoperabilidad.

O2. Identificar el tipo de soluciones potenciales genéricas que se pueden aplicar. Identificación de distintas estrategias para la habilitación de interoperabilidad universal entre sistemas.

O3. Identificación, diseño y desarrollo de habilitadores digitales que permiten soluciones de interoperabilidad a distintos niveles (técnico, sintáctico y semántico) en distintos niveles del sistema o plataforma IoT (dispositivo, red IoT, middleware, aplicación), con especial atención sobre el nivel de plataforma IoT (middleware o aplicación).

O3.1 Mejora innovadora de la capacidad de proporcionar interoperabilidad técnica de redes y protocolos de transporte

O3.2 Obtención de interoperabilidad de plataforma IoT (sintáctica y semántica) mediante el uso de estándares

O3.3. Habilitación de interoperabilidad entre plataformas IoT heterogéneas (sintáctica y semántica) mediante el uso de soluciones novedosas

O4. Implementación de las distintas soluciones de interoperabilidad

O5. Aplicación de las distintas soluciones en casos reales en distintos dominios de aplicación y validación.

1.5. Estructura de la tesis

A continuación se detalla el contenido de cada capítulo y su relación con los objetivos de la tesis:

Capítulo 1- Introducción

En este capítulo se introduce el marco de investigación de esta tesis, la motivación subyacente, conceptos clave para la comprensión del trabajo

realizado en esta tesis doctoral,, la interoperabilidad de los dispositivos físicos en el Internet de las cosas, que es el objeto de estudio de esta tesis. También se listan las principales contribuciones realizadas, tales como publicaciones y participación en proyectos de investigación, se describen los objetivos de la investigación de esta tesis y se presenta su estructura. La primera parte de este capítulo guarda relación con el objetivo O1.

Capítulo 2- Interoperabilidad en IoT

Este capítulo explica en detalle el problema de la interoperabilidad en IoT, y su situación actual, los grandes beneficios potenciales de su habilitación, los grandes impedimentos que tiene su habilitación y los tipos de soluciones existentes y sus limitaciones. Pone especial atención hacia la interoperabilidad semántica entre plataformas heterogéneas y su integración horizontal. Constituye un estado del arte en sí de la interoperabilidad en los sistemas IoT. El capítulo está relacionado con el objetivo O1 y O2.

Capítulo 3 – Interoperabilidad técnica en el Internet del Futuro: control inteligente de la congestión y Multipath TCP.

En este capítulo se aborda el tema de la interoperabilidad técnica y de la Internet del Futuro, presente en la futura Nueva Generación de Internet de las Cosas. Se da una visión general del problema del tráfico creciente en las redes y la gran preocupación actual por el riesgo de colapso inminente y degradación de servicio, impidiendo o disminuyendo notablemente la capacidad de proporcionar interoperabilidad técnica de las redes y otros habilitadores como protocolos de transporte. Con el fin de minimizar este problema y maximizar esta capacidad, se diseña, implementa y evalúa un control de congestión muy innovador para el protocolo MPTCP con capacidades muy notables para la optimización del uso eficiente de las redes y mejora significativa de la congestión, no solo a nivel local sino global, e inclusive capaz de mantener la conexión cuando un camino de red cae. Se corresponde con los objetivos O3.1, O3, 04 especialmente y O5 desde el punto de vista de evaluación.

Capítulo 4- Interoperabilidad entre sistemas por adhesión a estándares: sistema AAL para la gestión de residencias

En este capítulo se estudia el enfoque de la habilitación técnica, sintáctica y semántica mediante el uso de estándares abiertos. En esta línea, se crea un sistema para la gestión AAL de residencias que integra un Servicio de Observación de Sensores y múltiples servicios AAL, permitiendo la integración horizontal de sensores, solucionando el problema de "vendor lock-in" y proporcionando interoperabilidad entre sistemas afines por uso de estándares y modelos comunes. Cubre los objetivos O3.2, O4 y O5.

Capítulo 5 - Interoperabilidad semántica entre plataformas heterogéneas

En este capítulo se estudia una nueva estrategia para la consecución de la interoperabilidad entre plataformas y sistemas IoT heterogéneos a todos los niveles, gracias a una novedosa arquitectura de interoperabilidad basada en capas, proporcionando soluciones de interoperabilidad a cada una de ellas (dispositivo, red, middleware, semántica, aplicación), en el marco del proyecto INTER-IoT. En concreto, este capítulo se centra especialmente en el traductor semántico en tiempo real capaz de proporcionar interoperabilidad semántica universal entre cualquier par de plataformas heterogéneas.

Capitulo 6 – Habilitación de la interoperabilidad semántica en ecosistema AHA de plataformas IoT

Este capítulo describe la aplicación de las soluciones de interoperabilidad entre múltiples plataformas heterogéneas en un caso real a gran escala en el dominio de Envejecimiento Activo y Saludable (AHA). Para ello se utiliza una suite de interoperabilidad cuyo elemento central es el traductor semántico universal funcionando conjuntamente con el middleware de interconexión de plataformas de INTER-IoT, además del desarrollo de alineamientos semánticos entre plataformas y puentes de comunicación para plataformas. Se describe la arquitectura de interoperabilidad, los elementos desarrollados, el caso de uso de

interoperabilidad a gran escala creando un ecosistema IoT AHA europeo, y su validación.

Capítulo 7 Conclusiones

En este capítulo se recogen las conclusiones generales de la investigación.

Capítulo 2

Interoperabilidad en Internet de las Cosas (IoT)

"Todas las personas y las cosas están interconectadas en una especie de matriz"

Max Planck

2.1. Introducción

La interoperabilidad se refiere a la capacidad de los sistemas y componentes para comunicarse y compartir información entre ellos de forma efectiva. En el área de IoT, esta característica crucial es clave para liberar todo el potencial del paradigma de la IoT, que incluye inmensos beneficios tecnológicos, económicos y sociales aún sin explotar. Hay que destacar que la interoperabilidad de IoT también tiene una importancia significativa en el análisis de Big Data, y en el Edge y Cloud Computing [13] y en consecuencia también en el análisis de Inteligencia Artificial como Machine Learning o Deep Learning [14], porque facilita muy significativamente el procesamiento de datos y permite una mejora potencial del valor asociado a los datos (dato enriquecido). Por ello, tiene una importancia significativa en la digitalización de nuestro mundo y sobre la aplicación y efectividad de los habilitadores digitales de la Industria 4.0 [15].

Desafortunadamente, la interoperabilidad se considera el mayor reto técnico al que se enfrenta la IoT en la actualidad, junto a la seguridad. Esto se debe principalmente a la falta de un estándar de referencia establecido globalmente, cuya existencia no se prevé en el futuro, y a la vasta heterogeneidad intrínseca de los sistemas de IoT a

todos los niveles [1]. La situación actual en IoT refleja una falta general de interoperabilidad entre sistemas y plataformas, muy distante de la visión del paradigma en que los objetos inteligentes de podrán conectarse de manera transparente y automática en cualquier lugar, sin ninguna barrera técnica de interoperabilidad. La realidad actual es que los sistemas IoT, gestionados por plataformas IoT, representan silos verticales incapaces de compartir información, interoperar y cooperar entre ellos [7]. Esta fragmentación en el ecosistema global IoT causa numerosos problemas económicos y técnicos, limita el uso de la información e impide el establecimiento de sinergias [5].

El objetivo de esta tesis doctoral es la investigación del difícil reto que constituye la habilitación de interoperabilidad en IoT, y el diseño, desarrollo, implementación y uso de diversas herramientas tecnológicas (habilitadores digitales) para conseguir establecer interoperabilidad a distintos niveles entre diferentes plataformas IoT heterogéneas.

En el marco de esta tesis, este capítulo constituye una introducción a conceptos clave necesarios para la comprensión del trabajo realizado, además de proporcionar un análisis del estado del arte respecto a la interoperabilidad en IoT. Se introduce el concepto de interoperabilidad en el área de IoT y sus distintos niveles (técnico, sintáctico y semántico), se describe los grandes retos técnicos a los que se enfrenta su consecución y la situación actual en el paradigma de IoT respecto la interoperabilidad. De manera general, se hace un análisis a posibles soluciones para habilitar interoperabilidad, tanto intra-sistema como inter-sistema.

2.2. Internet de las Cosas

Internet de las Cosas (IoT) [16] es un reciente paradigma tecnológico que está transformando y revolucionando el mundo en el que vivimos. A pesar de que tan solo hemos empezado a vivir una fase inicial y meramente arañado su potencial son innegables los cambios profundos que ha provocado en nuestra sociedad, industria y economía, y su papel en la digitalización o transformación digital de nuestro mundo. Sin embargo, actualmente para poder desplegar todo su potencial aún hace falta abordar y resolver grandes retos tecnológicos asociados.

IoT se entiende como un nuevo paradigma que algunos autores consideran una evolución natural de la Internet [17], que responde a un mundo hiperconectado en el que objetos inteligentes ("cosas") están conectados masivamente a Internet, enviando información a servicios u otros dispositivos, o bien recibiendo información. El término de "Internet de las Cosas" responde al hecho de que las entidades conectadas a Internet no son mayoritariamente "objetos" o "cosas", dispositivos muy simples con capacidad de conexión y recursos limitados que contrastan con las típicas máquinas de grandes capacidades conectadas mayormente en Internet antes de la llegada de la IoT: los ordenadores [18].

Estas "cosas" son típicamente sensores o actuadores de pocos recursos de procesamiento, energía y almacenamiento, con capacidad de conectividad a la red, que en general monitorizan su entorno o registran una acción. No obstante, dentro de estos objetos conectados también se incluyen programas software y dispositivos más complejos como teléfonos inteligentes.

Las numerosas definiciones que se han dado de la IoT desde un punto de vista tecnológico, están de acuerdo con las siguientes características:

- presencia de una infraestructura de red global o de conectividad de red, que permite la interoperabilidad de los elementos de una IoT, su integración y un esquema de direccionamiento único. Se concibe como necesaria una infraestructura global cualquiera (no necesariamente basada en IP) que permita soportar una red separada de las Cosas.
- Los objetos cotidianos, y no sólo los dispositivos TIC, como ordenadores, son los que tienen el papel protagonista en la IoT. Estos dispositivos o cosas tienen que ser legibles, reconocibles, localizables, direccionables y controlables.
- Tiene gran importancia el diseño de interfaces de comunicación eficaces entre los humanos y las cosas, o solamente entre cosas.
- Necesidad y existencia de soluciones que permitan vincular los objetos físicos y virtuales. Los sensores y actuadores están integrados en objetos físicos, siendo gestionados a través de sus representaciones virtuales dentro de un sistema de información digital superpuesto (plataforma IoT).

- Necesidad de asociar servicios a los objetos para el uso de la información IoT recogida por estos. Estos servicios pueden ser elementales o muy complejos.
- Los objetos inteligentes son generalmente autónomos. La complejidad de los sistemas puede controlarse mediante la consecución de la autogestión (autonomía).
- Heterogeneidad de las tecnologías subyacentes. Esto implica la necesidad de diseño de soluciones adecuadas que permitan la coexistencia de estas tecnologías dentro de la plataforma de interconexión IoT elegida.

La Internet de las Cosas ha tenido un crecimiento imparable en los últimos años, superado en número de objetos conectados al número de usuarios humanos conectados a Internet, así como al número de ordenadores. El paradigma de IoT está en constante evolución [19] y se diferencian tres olas o generaciones:

1ª generación : en esta primera etapa destacan hitos técnicos que sientan las bases del funcionamiento básico de la Internet de las Cosas:

- -Objetos etiquetados (uso de un identificador único para cada objeto en una plataforma). Esto permite identificar al objeto en plataformas de gestión.
- -Definición de arquitecturas de referencia para las comunicaciones Máquina a Máquina (M2M) [20]
- -Integración de la tecnología RFID con las Redes de Sensores Inalámbricas.

2ª generación*:* destacan hitos importantes en relación con la web semántica y las redes sociales.

- Web de las Cosas (Web of Things) – Los dispositivos de recursos limitados o cosas participan en las comunicaciones web.
- Servicios de redes sociales en los que se comparte información IoT: Permitir que las personas compartan los datos generados por sus objetos inteligentes con personas que conocen y en las que

confían, aprovechando los servicios de redes sociales humanas existentes

- Internet social de las cosas Hacer que los objetos puedan participar en comunidades de objetos, crear grupos de interés y realizar acciones colaborativas con el objetivo de facilitar el descubrimiento de servicios e información
- -Semántica: uso de una descripción de las características de los objetos de la IoT para fomentar la interoperabilidad de los sistemas

3ª generación: era de IoT de los objetos sociales, la integración con la nube, la computación en la nube y el uso de internet del futuro.

En la actualidad nos encontramos en la tercera generación, camino a la nueva generación de IoT [11] o Internet del Futuro [16]. Se prevé un futuro despliegue total del paradigma, donde los objetos podrán conectarse ubicuamente de manera transparente y automática en cualquier lugar, y además de enviar información o recibirla, estar interconectados e interactuar entre ellos.

2.2.1. Descripción general de un sistema IoT

Un sistema IoT está compuesto en su nivel más bajo por objetos inteligentes o cosas, que son en su mayoría sensores y actuadores con capacidad de conexión a Internet. Este sería el nivel más bajo o capa de dispositivos. La información recogida por estos sensores es enviada a servicios, aplicaciones o plataformas de gestión IoT en una capa superior a través de Internet. La conectividad de estos objetos inteligentes es típicamente inalámbrica (aunque existen sensores y otros dispositivos inteligentes cableados) y utiliza tecnologías de baja potencia y bajo alcance debido a los pocos recursos energéticos de los que disponen. Esto implica que generalmente es necesario el uso de pasarelas de red específicas para IoT [7] que permitan la conexión a Internet a través de ellas de objetos inteligentes con conectividad de corto alcance. La capa de red estaría compuesta por la red IoT (o típicamente red en la que se conectan los objetos a la pasarela inteligente de red) y ya propiamente la conexión de

la pasarela a Internet, en donde se encuentran los servicios a los que se envían estos datos (que suelen ser gestionados de manera intermedia, antes del servicio, por una plataforma IoT).

Las plataformas de IoT [21] gestionan los datos enviados por los objetos inteligentes, y los envían a la capa de servicios y aplicaciones que utiliza estos datos. El análisis inteligente de esta información masiva por parte de Inteligencia Artificial o métodos Machine Learning se realizaría en esta capa superior por norma general.

2.3. Interoperabilidad

A pesar de las distintas definiciones que existen de interoperabilidad dadas por organismos técnicos y miembros de la comunidad científica coinciden en el significado general de este concepto y en las condiciones necesarias y suficientes para lograrlo: "La interoperabilidad puede entenderse como la capacidad de intercambiar información entre varias entidades y la capacidad de utilizarla"[7] .

Así pues, se entiende como interoperabilidad la capacidad de entidades (ej. sistemas, plataformas, aplicaciones o incluso componentes) para establecer comunicación e intercambiar información entre ellas siendo capaces de entender y utilizar efectivamente esta información recibida [5].

El concepto de interoperabilidad comprende diferentes niveles o tipos de interoperabilidad según el grado en que se efectúa el intercambio y la comprensión de información. En este sentido, existen tres niveles de habilitación de interoperabilidad [7]:

-**Interoperabilidad técnica**: Este tipo de interoperabilidad está referido a la capacidad de dos sistemas o entidades de establecer comunicación entre ellos e intercambiar mensajes [22]. No implica que estos mensajes puedan ser correctamente leídos, haya conocimiento del formato de datos empleado o se entienda el significado de los datos recibidos. La interoperabilidad técnica está estrechamente relacionada con los elementos que permiten una comunicación de máquina a máquina (M2M) [23]; entre ellos tienen especial relevancia los protocolos de comunicación, y la infraestructura necesaria para establecerla (tanto hardware como software, siendo muy relevantes

las interfaces de comunicación). Requiere de la existencia de conectividad entre los sistemas.

-**Interoperabilidad sintáctica** [24]: Implica que los datos intercambiados entre sistemas pueden ser correctamente leídos por el receptor, independientemente de que entienda o no su significado. Se refiere a la capacidad de los sistemas de interpretar correctamente la estructura de los mensajes y datos intercambiados y, por lo tanto, ser capaces de leer su contenido aunque no sean conscientes del significado de esta información. La interoperabilidad sintáctica se apoya en el uso de formatos de datos, ya que los mensajes intercambiados entre los sistemas requieren una representación de datos común para la correcta interpretación de la estructura y el contenido de los datos. El uso de formatos de datos estandarizados evita la ambigüedad en la interpretación y representación de los datos. Ejemplos de formatos de datos son estándares tales como, XML, JSON o CSV, que proporcionan una sintaxis de alto nivel. Para conseguir esta interoperabilidad, los sistemas deben ser conscientes de en qué formato de datos reciben y deben decodificar la información. Un ejemplo de interoperabilidad sintáctica sería un sistema que recibe información de otro y es capaz de reconocer correctamente su formato de datos específico (por ejemplo, CSV) y por ello, de extraer correctamente los datos del mensaje (por ejemplo, un conjunto de valores). No tiene por qué ser consciente de lo que estos datos representan (por ejemplo, litros de lluvia), siendo así incapaz de utilizar los datos dentro del contexto correcto.

-Interoperabilidad semántica: Implica que los sistemas son capaces de entender el significado de la información recibida, y por ello, capaces de utilizarla efectivamente. Se considera el nivel más elevado de interoperabilidad, y es necesaria para la cooperación y coordinación entre sistemas. Esta interoperabilidad implica la comprensión automática e inequívoca de la información recibida [25]. Para poder conseguirse interoperabilidad semántica entre sistemas es necesario conseguir previamente interoperabilidad sintáctica y técnica. También es necesario que el receptor sea capaz de entender el modelo semántico de información en que están expresados los datos, de forma automática y no ambigua. Elementos como ontologías, tecnologías semánticas y sistemas de gestión del conocimiento son medios que facilitan su habilitación. En el ejemplo dado en el párrafo anterior, si existe

interoperabilidad semántica el sistema sería capaz de entender que los valores son litros de agua caídos en días determinados, y podría utilizar esta información para, por ejemplo, realizar predicciones de probabilidad de lluvia en días venideros.

2.4. Situación actual de la interoperabilidad en IoT

2.4.1. Importancia de la interoperabilidad

En IoT, la interoperabilidad desempeña un papel esencial, hasta el punto de que se considera que probablemente no haya ningún otro ámbito tecnológico en el que la interoperabilidad sea tan crítica y relevante como en el caso de IoT [Foro Económico].

En esta línea, según un estudio realizado por el McKinsey Global Institute [26], sin interoperabilidad no se puede obtener al menos el 40% de los inmensos beneficios potenciales de la IoT.

Desde un punto de vista intra-sistema, debido a que los sistemas IoT implican la interconexión e interoperación de múltiples elementos, la interoperabilidad constituye una necesidad imperativa dado que es esencial que puedan interoperar entre ellos. La interoperabilidad es indispensable para que cualquier conjunto de dispositivos intercambie información y trabaje de forma conjunta, actuando como un verdadero sistema de IoT.

Por otro lado, la interoperabilidad entre sistemas IoT tiene una importancia crítica en el contexto tecnológico, económico y social actual [6]. Esta interconexión de sistemas propicia que se compartan datos relevantes y se establezcan importantes sinergias, mejorando la calidad de la información, la calidad del servicio y la experiencia proporcionada al usuario. Además, la interoperabilidad de la información entre diferentes sistemas enriquece la analítica de Big Data mediante el modelo 3v [13] a través de la integración de una variedad de formatos, modelos y definiciones de datos, en un modelo de datos común para aumentar su eficacia. De hecho, uno de los principales retos de Big Data es manejar adecuadamente esta diversidad de datos [27].

La conexión de los dispositivos inteligentes IoT genera conocimientos inesperados y un importante valor intrínseco que será positivo para la ciudadanía y el sector

industrial [28]. Sin embargo, como ya se ha mencionado anteriormente, [26] sin una interoperabilidad adecuada en los sistemas de IoT, no será posible alcanzar sus beneficios potenciales de IoT.

Actualmente en IoT, la insuficiente interoperabilidad entre plataformas produce importantes problemas tanto a nivel técnico como empresarial. Se considera un problema tecnológico de bloqueo que provoca importantes contratiempos tecnológicos [5]. Los problemas más típicos son:

- la imposibilidad de integrar determinados dispositivos de IoT en determinadas plataformas. Hay que notar que en el caso de plataformas IoT propietarias es general el fenómeno "vendor lock-in", en el que las plataformas no permiten o tienen fuertes restricciones a la inclusión de objetos inteligentes de un fabricante distinto, limitando de manera importante los tipos de dispositivos IoT que se pueden incluir en un sistema y por tanto, el potencial de este a la hora de poder diseñar y proporcionar soluciones IoT. En cualquier caso, los problemas de integración de ciertos dispositivos no son exclusivos de plataformas propietarias.
- la incapacidad de desarrollar aplicaciones y servicios sobre varias plataformas y diferentes dominios a la vez, ya que las aplicaciones son específicas para las interfaces, protocolos de comunicación y modelos de datos e información de la plataforma que les proporciona.
- la existencia de "silos verticales" o sistemas que no pueden compartir la información que gestionan con otros, limitando el uso de esta información y la generación de valor añadido, o la posibilidad de cooperación y valiosas sinergias entre sistemas. El actual ecosistema global de IoT está muy fragmentado debido a que coexisten muchos sistemas verticales. Debido a la ausencia de interoperabilidad entre ellos, estos sistemas se mantienen como silos verticales aislados de información que no pueden interoperar, colaborar o compartir información específica [29]. Típicamente hay una fragmentación por dominio de aplicación. Estos sistemas verticales no pueden beneficiarse de las sinergias y oportunidades que surgen como fruto de la interoperabilidad de los sistemas. Esto tiene importantes desventajas desde un punto de vista técnico y económico y afecta a la calidad de los servicios ofrecidos al usuario.

- escasa penetración de la tecnología IoT debido a que se encuentra con barreras de interoperabilidad
- dificultad a la hora de crear soluciones IoT que utilizan múltiples fuentes
- mayor dificultad en el desarrollo de aplicaciones de IoT que explotan varias plataformas en diversos dominios.
- costes mayores, ya sea en términos de desarrollo como económicos, por no poder beneficiarse de una situación de interoperabilidad. Por ejemplo, el no poder integrar horizontalmente dispositivos en una solución IoT implica tener que buscar dispositivos más caros o formas de integración que implican un desarrollo costoso. A nivel de uso de modelos de información, por ejemplo, la dificultad de reuso de aplicaciones o soluciones de una plataforma a otra implica grandes costes de desarrollo en la creación de otras similares.
- baja o nula posibilidad de reuso de soluciones técnicas
- la falta de interoperabilidad tiene muchos inconvenientes relevantes para el desarrollo de aplicaciones y un enorme impacto en la calidad de los análisis de big data. La falta de interoperabilidad dificulta sustancialmente la integración de varias fuentes de datos del IoT para extraer información útil. La integración de diferentes fuentes de datos mejora los datos con información de contexto mediante el acceso, la combinación y la mezcla de varios conjuntos de datos; de esta manera adquieren mayor valor [Janssen]. Los datos enriquecidos permiten encontrar correlaciones, patrones, tendencias y establecer relaciones de causalidad.
- desde un punto de vista de adopción, el rechazo de los clientes y las empresas a emplear la tecnología IoT y la baja satisfacción de los usuarios. Además de la baja capacidad de reusabilidad de las soluciones técnicas ya mencionada.

La insuficiente interoperabilidad es el principal obstáculo para el desarrollo de la IoT y su adopción por el mercado [Sector Telecomunicaciones]. Esta situación de falta de interoperabilidad ralentiza significativamente la introducción a gran escala de la tecnología IoT.

Además, la falta de interoperabilidad ralentiza e incluso impide la incipiente evolución de la IoT. Los entornos inteligentes ambientales requieren una interoperabilidad sin fisuras entre los elementos y las interfaces. Asimismo, la interoperabilidad es esencial

para la creación de interfaces naturales y transparentes (orientadas al ser humano) de los sistemas inteligentes. También tiene una importancia vital para la integración de la IoT con la Inteligencia Artificial y la inclusión de nuevos mecanismos como la seguridad de la cadena de bloques. Por otro lado, la visión de futuro de la IoT, o visión del paradigma completamente desplegado, prevé que todos los dispositivos con capacidades de comunicación y detección puedan interconectarse e interactuar de forma transparente [19][30]. Para poderse llevar a cabo la interoperabilidad desempeña un papel fundamental, ya que esta integración sin fisuras y completamente transparente requeriría un grado muy alto de interoperabilidad a todos los niveles. A día de hoy construir un ecosistema global de dispositivos capaces de conecten entre sí automáticamente y de forma transparente es prácticamente imposible debido a las barreras de la falta de interoperabilidad.

2.4.2. Causas de la falta general de interoperabilidad

A pesar de los grandes beneficios de la habilitación de la interoperabilidad, actualmente es uno de los desafíos técnicos más difíciles a resolver en IoT. La interoperabilidad se considera el mayor reto técnico actual del paradigma de IoT, conjuntamente con la seguridad.

Actualmente los diferentes sistemas de IoT son típicamente incapaces de comunicarse entre sí o de interoperar en general [5], siendo la heterogeneidad y falta de interoperabilidad la condición general.

Esto es debido a la naturaleza altamente heterogénea de los sistemas de IoT y a la falta de un estándar global. El Internet de las cosas abarca una amplia gama de dispositivos, protocolos, tecnologías, redes, middleware, aplicaciones, sistemas, formatos de datos y modelos de información que presentan una gran diversidad. La heterogeneidad de las tecnologías subyacentes dificulta enormemente la interoperabilidad de los objetos y sistemas inteligentes, ya que siguen reglas y estándares diferentes. Desde el punto de vista de la información, la gran heterogeneidad en su representación siguiendo modelos semánticos de información completamente dispares, y el uso de multitud de formatos y estructuras de datos para soportarla, hace casi imposible que sistemas no diseñados inicialmente para interoperar entre ellos puedan entender el significado de los datos que intercambien.

En este sentido, la existencia de un estándar de referencia global para el IoT facilitaría notablemente la interoperabilidad al dotar de reglas y cierta homogeneidad a este universo heterogéneo. Sin embargo, actualmente no existe un estándar global de referencia de facto, lo que supone un problema importante a la hora de diseñar nuevos sistemas de IoT [31]. En su lugar existe una miríada de estándares compitiendo entre ellos, muy distintos entre sí, y no se prevé que en un futuro se establezca uno *de facto* sobre todos los demás [32].

Otro inconveniente que suma complejidad a la habilitación de interoperabilidad es el hecho de que la información de IoT típicamente fluye en flujos masivos de datos en tiempo real (IoT Big Data). La gestión y el procesamiento de estos datos, por su cantidad y velocidad, tiene una alta complejidad inherente [33].

Dentro de los distintos desafíos relacionados con la interoperabilidad en IoT, la comunicación e intercambio de información entre plataformas IoT es especialmente compleja y difícil de conseguir. Esto se debe mayormente a la gran heterogeneidad entre los distintos modelos de información utilizados entre ellas, haciendo imposible la comprensión de la información en la comunicación directa y muy complicado cualquier intento de adaptación de los datos a otro modelo. Normalmente, los modelos de información se crean de forma independiente en los sistemas, por lo que no pueden comunicarse y compartir información con otros sistemas. Cada instancia de plataforma IoT (que no tipo de plataforma) utiliza sus propios estándares, formatos, ontologías y modelos de datos, siguiendo maneras completamente diferentes de representar la información. Poniendo un símil se podría decir que sería similar a la necesidad traducción de idiomas automática en nuestro mundo, lo que requeriría un intérprete formado o un software de traducción de idiomas, que generalmente no hacen traducciones perfectas debido a los matices y diferencias difíciles de generalizar entre ellos. Pero a diferencia de los idiomas actuales, en términos de plataformas IoT los modelos de información posibles se pueden considerar infinitos y son además altamente heterogéneos sin generalmente seguir "raíces" o estructuras comunes entre ellos, o tener equivalencias perfectas.

Además de la necesidad de entender el modelo de información, el reto más complejo, la interoperabilidad entre plataformas requiere de la comprensión sintáctica correcta de los datos y conseguir comunicación efectiva entre ellas a pesar de poder tener

interfaces dispares y distintas formas de establecer la comunicación e intercambiar información.

Por tanto, el mayor reto para la habilitación de la interoperabilidad de más alto nivel (interoperabilidad semántica) entre sistemas gestionados por plataformas IoT es el entendimiento de los modelos semánticos de información. Además de su heterogeneidad, falta de alineamiento parcial o total a ontologías o estándares de referencia en muchos casos, hay que añadir la dificultad de tener que tratar una gran mayoría de modelos de datos que no tienen soporte RDF o OWL, es decir, no se ha definido su estructura semántica y relaciones de triples [34][35].

Hay que destacar que la interoperabilidad entre plataformas es un terreno poco explorado en IoT, a pesar de los muchos alicientes y beneficios potenciales que ofrece, debido probablemente a su gran complejidad. Fuera de los esfuerzos realizados en la creación de ontologías y definición de buenas prácticas en su uso, la literatura no muestra muchas iniciativas en esta línea. Destacan esfuerzos de investigación abordando el problema de la interoperabilidad entre plataformas por parte de iniciativas europeas, los cuales se verán en un próximo apartado [29].

2.5. Soluciones potenciales para la habilitación de interoperabilidad

Desde un punto de vista intra-sistema, destacan dos soluciones de interoperabilidad que permiten salvar, en la medida de sus posibilidades específicas, distintos obstáculos para la conectividad de objetos inteligentes y para el flujo y gestión de la información que recogen. Estas soluciones serían las plataformas de IoT, que permiten la gestión de la información IoT de la capa de sensores y actuadores, y las pasarelas inteligentes IoT de red, que permiten a dispositivos IoT con teconologías de comunicación de corto alcance conectarse a las redes.

Las primeras, las plataformas IoT, permiten la gestión de los datos provenientes de la capa de dispositivos IoT conectados a ellas dentro de su propio modelo de datos y formato de información. Esto permite la creación de un pequeño ecosistema con aplicaciones y servicios asociados.

Las segundas, las pasarelas de red inteligentes, permiten que dispositivos IoT de conectividad de bajo alcance puedan enviar sus datos a servicios, plataformas, o sistemas en una capa superior. Las tecnologías de comunicación inalámbricas de muchos dispositivos IoT, debido a su corto alcance y baja potencia no les permiten conectarse directamente a Internet y deben hacerlo a través de un elemento intermedio. Además, sus datos suelen requerir algún tipo de preprocesado y es necesario gestionar y convertir protocolos de comunicación.

Por otro lado, para la habilitación la interoperabilidad intra-sistema, entre distintas plataformas IoT tienen especial relevancia los modelos de información y la semántica. En este sentido, para facilitar la representación de la información IoT, el uso de modelos de información afines, la homogeneización de los modelos de información y la comprensión inequívoca de términos y conceptos, se han hecho grandes esfuerzos en el desarrollo y uso de ontologías que recogen de manera no ambigua la representación de información contextual de modelos semánticos especialmente diseñados para la IoT y dominios específicos de aplicación. También, en la misma línea, se ha hecho un esfuerzo en la identificación de buenas prácticas para el uso y reuso de ontologías que prevengan una innecesaria heterogeneidad en los modelos semánticos ofrecidos y empleados en el paradigma de IoT.

Desafortunadamente, respecto a la interoperabilidad entre sistemas hay mucho camino por recorrer debido a su gran complejidad inherente y dificultades asociadas. La mayoría de esfuerzos están dirigidos al desarrollo, catalogación y uso de ontologías, facilitando modelos semánticos que pueden ser reutilizados. Se ha explorado poco el desarrollo de soluciones de interconexión e interoperabilidad entre sistemas heterogéneos. En general, estas soluciones son ad-hoc, limitadas a los sistemas concretos que interconectan, parciales y con escasa capacidad de crecimiento y poca o nula escalabilidad, y típicamente están enfocadas solamente al nivel de datos o aplicación. Muy pocas iniciativas han explorado la construcción de soluciones genéricas, escalables y reutilizables o que aborden el problema de la interoperabilidad en diferentes capas de los sistemas IoT. Las diferentes propuestas para abordar la interoperabilidad en IoT provienen de iniciativas comerciales y soluciones basadas en los intentos de normalización de los diferentes organismos de estandarización, así como también del resultado de proyectos públicos de investigación. Dentro del marco

de proyectos de investigación, destacan las iniciativas de iCore y Butler [19] que diseñaron plataformas IoT diferentes pero interoperables entre sí por diseño. Otros esfuerzos destacables son iniciativas FP7 H2020 que proporcionan herramientas y desarrollos para tratar de facilitar interoperabilidad entre los sistemas a distintos niveles y con enfoques muy diferentes. Estas serían BigIoT [36], SymbIoTe [37], Vicinity [38] e INTER-IoT [39], entre otras. Otras investigaciones relevantes son WSO2 [40], FIESTA-IoT [41] y OpenIoT [42]. Los principales esfuerzos de interoperabilidad de estas soluciones se suelen centran en la semántica y en las interfaces de programación de alto nivel para la capa de aplicación. Entre estas soluciones destaca el conjunto de herramientas proporcionado por INTER-IoT bajo el objetivo de permitir la habilitación de interoperabilidad en cada una de las capas de los sistemas IoT, de las que se hablará en un próximo capítulo.

Existen dos enfoques principales para hacer posible la interoperabilidad semántica en los sistemas y plataformas IoT :

1) el uso estándares comunes. En concreto, respecto al nivel de modelos de información, el uso de ontologías semánticas para una utilizar una representación común de la información, lo que facilita hasta cierto punto la interoperabilidad
2) la aplicación de soluciones técnicas entre sistemas no interoperables o sobre ellos, que usan un enfoque de adaptación de elementos.

Interoperabilidad por uso de estándares (sistemas y plataformas IoT afines)

Este es el caso de que distintos sistemas estén de acuerdo en utilizar un estándar o conjunto de reglas para su comunicación que permite la correcta interpretación de la información. Esta alineación habilitaría la interoperabilidad semántica entre ellos.

En el caso concreto del modelo de información, la consecución de interoperabilidad semántica los esfuerzos en su gran mayoría están enfocados al uso de ontologías, para permitir utilizar un modelo común. Las ontologías son documentos que recopilan el significado y definición de clases representando conceptos y su relación con otros elementos. Hay que notar que esta no es la única posibilidad del uso de ontologías,

como se puede ver en soluciones que aplican adaptación de modelos semánticos, por ejemplo, pero sí la forma en que fundamentalmente son utilizadas.

Se considera que un estándar global de facto para IoT podría ayudar en gran medida a solucionar el problema de interoperabilidad en IoT, proporcionando una serie de referencias a las que los sistemas se intentarían alinear [32]. Sin embargo, este estándar no existe, y hay en su lugar una miríada de estándares "locales" compitiendo, sin que ninguno predomine claramente sobre todo el conjunto. Esta situación hace suponer que la existencia de un estándar global es difícilmente factible en el futuro, tanto a medio como a largo plazo [5].

Interoperabilidad por adaptación de formatos, modelos de información y ajustes

Los esfuerzos de investigación para lograr la interoperabilidad semántica suelen centrarse en el uso de ontologías comunes entre los sistemas que pretenden interoperar [25]. Sin embargo, este enfoque no suele ser viable entre sistemas que no fueron diseñados inicialmente para interoperar [43] y que, por tanto, no comparten estándares comunes. El esfuerzo de cambiar la semántica en una plataforma IoT establecida es, en general, muy costoso en términos de desarrollo, especialmente una vez que se construye un ecosistema de aplicaciones encima, ya que implicaría adaptarlas a la nueva semántica. Además, en muchos casos, esto ni [35] siquiera es posible si la plataforma no es compatible con el formato de datos de destino. En estos casos solo son viables soluciones que impliquen el cambio o ajuste de los mensajes enviados o recibidos para que su información pueda ser utilizada, o inclusive ajustes en el receptor. Estas soluciones son ad-hoc para un caso concreto entre dos sistemas, y se pueden entender como un ajuste para poder realizar algún tipo de interacción necesaria. La única herramienta actualmente que permite la traducción semántica de mensajes en tiempo real entre modelos semánticos diferentes está vista en los capítulos 5 y 6 [35] [44], y se ha desarrollado en el marco del proyecto H2020 INTER-IoT [45].

A nivel de red y dispositivo, destacan las soluciones de conversión de formato, protocolos y de cambio de tecnología de comunicación que representan las pasarelas de red inteligente para IoT.

2.5.1. Estándares y Arquitecturas de referencia

Como se ha visto, un enfoque eficaz para abordar la interoperabilidad es el uso de estándares, modelos de arquitectura de referencia y la aplicación de las mejores prácticas en los despliegues de IoT. A continuación, se mencionan las normas más relevantes para IoT:

- **OneM2M:** es la iniciativa mundial de estándares para las comunicaciones IoT y Machine-to-Machine (M2M). OneM2M está trabajando en una capa de servicio que incluye requisitos técnicos, especificaciones de la interfaz de programación de aplicaciones (API), semántica de datos y soluciones de seguridad [46] [47].
- **AllJoyn :** Es un framework de código abierto impulsado por la AllSeen Alliance que permite que los dispositivos se comuniquen con otras máquinas independientemente de la tecnología de comunicación gracias al uso de un protocolo común [48].
- **IoTivity:** Es una iniciativa de la Open Connectivity Foundation. Su implementación en la nube da lugar a la plataforma con el mismo nombre [49]
- **ARM:** Es un modelo arquitectónico de referencia de IoT propuesto por el proyecto de investigación europeo IoT-A. Esta iniciativa de estandarización consiste en un conjunto de bloques de construcción que representan conceptos y componentes básicos que permiten la creación de sistemas IoT interoperables [50].

Otros grupos de trabajo también han aportado sus propias iniciativas de estandarización, como es el caso de las organizaciones UIT [51], ETSI [52] e IPSO Alliance [53].

Al existir un gran conjunto de estándares y la ausencia de un estándar global para IoT de facto, en este contexto multiestándar, aumenta la alta fragmentación y el

desarrollo de sistemas verticales de IoT, ya que los sistemas que operan con diferentes estándares no pueden comunicarse entre sí.

2.5.2. Pasarelas Inteligentes de Red para IoT

Las pasarelas de red para redes IoT tienen un papel muy importante respecto a la habilitación de interoperabilidad. Requieren de más capacidades y recursos que las pasarelas de red normales, cuyo papel se reduce a las funciones de enrutamiento y red tradicionales; las pasarelas inteligentes para redes IoT además deben ser capaces de proporcionar conectividad para muy diversos tipos de tecnologías inalámbricas (ej. ZigBee, LoRA, WiFi..), realizar conversión de protocolos (ej. MQTT por parte del sensor a TCP/IP en que lo recibirá la plataforma), conversiones sintácticas de formato de datos (cambio de un formato de datos usado por el objeto a otro en que se espera recibir la información en el otro extremo, ej. de JSON a CSV), o inclusive tareas de preprocesado y relleno de datos IoT incompletos. Por ello, tienen un papel clave a la hora de permitir la interoperabilidad entre la capa de sensores y los sistemas que reciben la información enviada y viceversa en el caso de actuadores. Habilitan la interoperabilidad técnica y sintáctica y pueden llegar a realizar tareas específicas para permitir la semántica (adaptación del formato de información).

Permiten que objetos inteligentes, típicamente con recursos energéticos y de procesamiento muy limitados, y tecnologías de conectividad inalámbrica de corto alcance puedan acceder a Internet y enviar datos a una plataforma de gestión IoT o a servicios que los utilicen en una capa superior.

Un ejemplo de pasarelas inteligentes son las pasarelas IoT definidas por software. Estas pueden implementarse en cualquier infraestructura hardware que tenga los requisitos mínimos necesarios en términos de potencia de procesamiento (por ejemplo, pueden instalarse en un procesador de bajo consumo, como una Raspberry). Algunos ejemplos relevantes de estas pasarelas son:

- **Eclipse Kura** [54]**:** Proyecto de código abierto de Eclipse que proporciona una plataforma para construir puertas de enlace de IoT. Kura ofrece una API de servicios y es capaz de gestionar eventos. Permite la gestión remota de las pasarelas IoT. Al estar basado en Java, Kura es independiente de la

plataforma (se ejecuta en cualquier plataforma). Como desventaja, no puede instalarse en dispositivos con memoria y potencia de procesamiento muy limitadas, ya que Java requiere recursos considerables.

- **Nodo intermedio de OneM2M** [55][48][56]**:** El nodo intermedio de una plataforma OneM2M actúa como una pasarela inteligente de IoT. El nodo intermedio OneM2M tiene una capa de servicio común que permite la interoperabilidad y el intercambio de datos. Esto se hace a través de las funciones de descubrimiento de dispositivos, gestión de la conectividad y establecimiento de conexiones seguras. Esta arquitectura puede ampliarse fácilmente desarrollando módulos específicos para nuevos dispositivos y protocolos.
- **Mihini** [57]**:** Es otro proyecto de código abierto de Eclipse que permite la interoperabilidad de dispositivos y el desarrollo de aplicaciones M2M. Este marco permite construir pasarelas inteligentes de IoT ligeras y portátiles, que requieren poca potencia de procesamiento.
- **Pasarela Intel IoT** [58]**:** Intel ofrece una pasarela IoT propia y una plataforma que permite su gestión remota. Además de la pasarela definida por software, Intel también proporciona el dispositivo físico. La pasarela Intel IoT puede conectar s un sistema IoT tanto dispositivos industriales relativamente antiguos (*legacy*) como objetos inteligentes modernos.
- **AGILE IoT** [59]**:** Es una pasarela modular de hardware y software concebida específicamente para el Internet de las cosas. Ofrece compatibilidad para la interoperabilidad de protocolos, dispositivos, los datos de los dispositivos y las aplicaciones de IoT, además de permitir la gestión de dispositivos conectados a ella.
- **BodyCloud** [60]**:** Una pasarela móvil inteligente pensada para instalarse en teléfonos móviles. Está diseñada con fines médicos para poder permitir la

monitorización de un conjunto de sensores médicos en el cuerpo de un paciente que lleva un teléfono inteligente con él.

2.5.3. Plataformas IoT

Una plataforma IoT [61] es un sistema software generalmente desplegado como un servicio web en un servidor, aunque puede estar desplegado en la nube como un PaaS (Plataforma IoT como Servicio). La plataforma monitorea y gestiona la información IoT procedente de objetos inteligentes conectados a ella, y proporciona esta información a aplicaciones y servicios que la utilizan en una capa superior. La plataforma gestiona esta información IoT usando su propio modelo semántico de información y formato de datos. Las aplicaciones y servicios por tanto, reciben y utilizan información IoT representada con esos modelos y estándares. Por esta razón, están asociadas a sus estándares específicos y a su modelo de información, creándose un sistema o microecosistema IoT en torno a ellos o dependiente de ellos.

Las funciones de la plataforma IoT son la recogida y gestión remota de datos IoT del conjunto de dispositivos inteligentes conectados, proporcionar puntos de acceso con conectividad para el envío o la recepción de datos y gestionar los objetos inteligentes asociados a ella.

En general, no es posible la comunicación directa entre diferentes plataformas de IoT, ya que emplean estándares, formatos de datos y semántica diferentes. Las plataformas pueden utilizar ontologías para definir la semántica subyacente de la información manejada en el ámbito de la plataforma o emplear en su lugar un modelo de datos predefinido. Estas representaciones de la información específicas de cada plataforma constituyen una compleja barrera de interoperabilidad entre diferentes plataformas, incluyendo la capa de aplicaciones y servicios asociadas a cada una de ellas, que no pueden utilizar información representada con otro modelo distinto. Por ello, una plataforma IoT junto con el conjunto de aplicaciones asociadas a ella representa un silo vertical de información IoT.

Se hace notar la diferencia entre un tipo de plataforma IoT (ej. FIWARE) y una instancia concreta de este tipo de plataforma respecto a modelos de información utilizados y ecosistema de aplicaciones asociado. Aunque puedan tener semejanzas

en los modelos de información empleados, las distintas instancias de una plataforma no utilizan como regla general el mismo, no siendo interoperables entre sí a nivel semántico, aunque en general sí utilicen el mismo formato sintáctico.

En la actualidad existen diferentes plataformas IoT, que representan la implementación de una arquitectura de interoperabilidad intra-sistema en particular. Los tipos de plataformas IoT de código abierto más importantes actualmente son:

- **FIWARE** [62], plataforma de código abierto nacida de una serie de proyectos I+D europeos. Es probablemente la plataforma de código abierto que goza de mayor aceptación y popularidad. El componente central de su arquitectura, el Orion Context broker, es el responsable de la orquestación de los mensajes que se producen entre los productores de información y los consumidores de esta. Por encima de este componente se encuentran los Generic Enablers, componentes de propósito general que a través de sus APIs y su conexión con otros proporcionan diferentes funcionalidades. Estas funcionalidades permiten la creación de Aplicaciones inteligentes basadas en el uso de IoT.
- **universAAL** [63] es una plataforma que permite la interoperabilidad de dispositivos, servicios y aplicaciones conectados a ella con la característica especial de utilizar en todas sus comunicaciones un modelo de información semántico complejo capaz de soportar triples, utilizando mensajes con formato RDF. Para la representación de la información utiliza una serie de ontologías para IoT y AAL que pueden ser extendidas. La parte central de la plataforma es un middleware adaptativo, que establece comunicaciones entre todos sus nodos para que puedan compartir información de contexto, de servicio y de interacción con el usuario. Ha sido diseñada para ser utilizada en entornos de Vida Asistida (AAL) con el fin de proporcionar soluciones AAL basadas en IoT.
- **OM2M** [64] es una plataforma de código abierto fruto de una iniciativa de Eclipse que constituye una implementación de la arquitectura para IoT

OneM2M [56], programa en Java utilizando bundles OSGI y que fue diseñada con un enfoque especial en la comunicación máquina a máquina (M2M).

- **sensiNact** [65] es una plataforma edge o plataforma-pasarela, ya que además de realizar las funciones de una plataforma IoT además permite la conexión directa de sensores a ella, y efectúa funciones de enrutamiento. Está orientada a servicios, ofreciendo su funcionalidad a través de diversos servicios disponibles. Las soluciones se construyen uniendo servicios de detección con servicios de actuación. Para facilitar la interoperabilidad, ofrece un modelo de datos genérico y extensible para facilitar la construcción de adaptadores para varios protocolos cuyo núcleo está formado por cuatro tipos de recursos: datos de sensores, actuación, variables de estado y propiedades.
- **IoTivity** [49] es un ejemplo de plataforma en la nube o PaaS (plataforma IoT como servicio). Es una iniciativa de la Fundación Linux que permite la conectividad de dispositivos IoT y sus datos, y su uso en aplicaciones por encima de ella con la particularidad de que toda la gestión se realiza en la nube.

Existen, a parte de las opciones de código abierto, un gran número de plataformas propietarias de código cerrado, las cuales típicamente presentan importantes restricciones en la integración de dispositivos y limitaciones al tipo de uso dado. Generalmente están asociadas a un fabricante importante de sensores IoT. Ejemplos de estos tipos de plataforma serían Waspmote [66] o Zatar [67]. Mención especial merece SOFIA2 [68], un tipo de plataforma propietaria basada en SOFIA, una plataforma de código abierto desarrollada en el marco del programa de investigación Horizonte H2020 de la Unión Europea.

2.5.4. Uso de Ontologías

Una solución para lograr la interoperabilidad semántica entre sistemas es el uso de una semántica común entre ellos. Esto soluciona la comprensión de información,

aunque puede haber otros aspectos como la sintaxis, o el establecimiento de comunicación y protocolo de intercambio de información que deben ser solucionados para poder habilitar completamente interoperabilidad hasta el nivel semántico. Las ontologías facilitan la habilitación de la interoperabilidad semántica y reducen la heterogeneidad en los formalismos de la IoT al proporcionar una definición formal del vocabulario y las reglas semánticas sobre un dominio particular [69], con el objetivo de unificar la representación de la información. Idealmente, la solución óptima sería el uso de un estándar global de facto para IoT (que abordara la comunicación y el ámbito semántico). Desgraciadamente, este estándar no existe y sería poco factible teniendo en cuenta la gran complejidad que supone y la rápida evolución del IoT y, por tanto, también de los conceptos del IoT a representar.

Además de la existencia de ontologías, deberían seguirse las mejores prácticas en cuanto a su uso y extensión para evitar, o al menos minimizar, la gran heterogeneidad que existe en la IoT en cuanto a modelos de información [69][34]. La comunidad de la Web Semántica recomienda encarecidamente realizar buenas prácticas para facilitar la consecución de la interoperabilidad en IoT mediante la reducción de la heterogeneidad subyacente entre las representaciones de la información en los sistemas [70] . Se trata, en primer lugar, de la reutilización de ontologías en la medida de lo posible. En segundo lugar, la creación de nuevas ontologías siguiendo las mejores prácticas. En concreto, se considera que la ontología SSN del W3C es la ontología general más adecuada para ampliarla y crear una nueva en un área específica relacionada con la IoT [71][35]. En tercer lugar, la definición de catálogos de ontologías para facilitar la reutilización y la creación de ontologías siguiendo las mejores prácticas [41].

Sin embargo, estas prácticas son generalmente ignoradas [72][9], y, en la actualidad, cualquier par de sistemas IoT que no hayan sido inicialmente diseñados para interoperar a nivel de información son generalmente incapaces de tener un entendimiento común de la información entre ellos. Además, la heterogeneidad en la representación de la información en la IoT es enorme y, por tanto, la complejidad de las posibles soluciones técnicas es elevada [73]. Otros grandes inconvenientes que dificultan la interoperabilidad en el panorama IoT actual son la necesidad constante

de actualizar las ontologías debido a la rápida evolución de la IoT y la falta de herramientas capaces de alinear las ontologías o las traducciones semánticas.

Ontologías importantes específicamente diseñadas para soportar y representar el tipo de información manejada en IoT son W3C SSN [71][74], SSN/SOSA [75],M3-lite [76][77], SAREF [78] y GOIoTP [79].

2.6. Conclusiones y remarques

En este capítulo se han visto conceptos clave para la compresión de este trabajo de investigación y se ha realizado una revisión exhaustiva del estado del arte actual respecto a la interoperabilidad en IoT. Este capítulo expone el resultado de la investigación y estudio del estado de la interoperabilidad en IoT, las necesidades actuales y soluciones potenciales (O1 y O2).

Aunque el trabajo de esta tesis doctoral trata la interoperabilidad a distintos niveles (técnica, sintáctica y semántica) en las distintas capas de los sistemas IoT y entre sistemas, está especialmente enfocada en la interoperabilidad semántica e interconexión middleware entre distintos sistemas y plataformas. En el capítulo 3 se trata el tema de la interoperabilidad técnica y el Internet del Futuro. En el capítulo 4 se estudia la habilitación de interoperabilidad intra-sistema y entre sistemas mediante la aplicación de estándares abiertos y modelos de información comunes, apoyada por la utilización de un Servicio de Observación de Sensores en el marco Web de Sensores (SWE). En el capítulo 5 se tratará el diseño, desarrollo, implementación y validación de soluciones de interoperabilidad innovadoras a todos los niveles entre plataformas IoT heterogéneas, con el enfoque de capas del proyecto INTER-IoT. Por último, en el capítulo 6 se verá la implementación de una suite de interoperabilidad, conteniendo varias de estas herramientas de interoperabilidad, en un caso real a gran escala europeo para el Envejecimiento Activo y Saludable.

Capítulo 3

Interoperabilidad técnica en el Internet del Futuro: Control inteligente de Congestión y Multipath TCP

"I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree that must be sure to span
So packets can reach every LAN.
First, the root must be selected.
By ID, it is elected.
Least-cost paths from root are traced.
In the tree, these paths are placed.
A mesh is made by folks like me,
Then bridges find a spanning tree."

Algorythme, Radia Pelmann

"El agua puede abrirse camino incluso a través de la piedra,
y si se ve atrapada siempre busca un nuevo camino.
Por ello siempre llega a su destino."

Memorias de una Geisha, Arthur Golden

3.1. Introducción: problema del aumento del tráfico de manera exponencial en redes

La utilización de las redes está creciendo de manera exponencial con la llegada y el vertiginoso crecimiento de la IoT. La Internet de las Cosas está sufriendo un crecimiento exponencial: la cantidad de dispositivos asociados se incrementa de manera multiplicativa año tras año. De acuerdo con la Corporación Internacional de Datos (IDC), el número de dispositivos inteligentes IoT o "cosas" conectados a Internet se estima que alcanzará los 41.6 billones en 2025, generando 79.4 zettabytes (ZB) . [80]. Debido a esta gran ocupación de las redes, la capacidad de las redes actuales será insuficiente dentro de unos años. A pesar del hecho de que las capacidades de las redes actuales se están aumentando progresiva y significativamente, este ritmo de mejora es insuficiente para satisfacer las crecientes necesidades debido al incremento exponencial del tráfico en las redes [81]. Con la llegada del 5G y el 6G se prevé que, a pesar de permitir la transmisión de grandes volúmenes de datos y el uso de un gran ancho de banda, por otro lado también incentivará el uso masivo de datos en las redes lo que tenderá a agravar este problema de tráfico [82].

Por estas razones el tema de la optimización de las redes está recibiendo una importante atención creciente por parte de la comunidad científica y las empresas proveedoras de servicio. Existe una urgente necesidad de diseñar y proporcionar soluciones eficientes para optimizar las redes de manera que se pueda reducir el impacto del tráfico generado por la IoT. Esto engloba aspectos como la utilización eficiente de los recursos de las redes [80] y un control de congestión eficaz y efectivo. Para ambos aspectos existe un gran potencial de mejora en cuestiones de eficiencia respecto a la situación actual y es un campo abierto a la investigación de nuevas formas de abordar estrategias y soluciones más efectivas y eficientes.

Obviamente, este problema latente de saturación de redes por insuficiencia de recursos y crecimiento exponencial del tráfico está directamente relacionado con la interoperabilidad técnica. La interoperabilidad técnica implica conectividad y posibilidad de conexión con otras entidades, lo cual habilita la posibilidad de poder interoperar a niveles superiores (sintáctico y semántico) en las redes si se cumpliesen los requisitos necesarios desde un punto de vista sintáctico y semántico. Por tanto,

un control de congestión eficiente que evita el colapso en la red y el uso óptimo de los recursos de red son factores que habilitan la interoperabilidad técnica.

Otro importante problema que enfrentar con la llegada del 5G en la Internet del Futuro es el tema de la limitación de energía en los dispositivos IoT [83]. Las “cosas” o dispositivos inteligentes IoT tienen la característica general de presentar limitaciones importantes en cuanto a la energía de la que disponen para su funcionamiento. El uso de 5G requiere un mayor gasto energético, y es una de las principales preocupaciones respecto al uso del 5G en teléfonos inteligentes [84]. El uso de múltiples interfaces y un control de congestión y uso de red eficiente ayudan significativamente a reducir el gasto energético [85]. Este problema energético también se infiere que existirá por extensión en 6G, donde ya se está estudiando el uso de una extensión de TCP, MPTCP, con fines de ahorro energético y de maximización de la velocidad de transmisión de datos [86], ya que permite la transferencia de grandes cantidades de datos en significativamente menos tiempo que una conexión TCP convencional. También, en esta línea, se está estudiando su uso conjunto con el protocolo WebRTC para permitir muy altas velocidades de transferencia de datos [87].

Por otro lado TCP, uno de los protocolos más importantes a nivel de transporte [88], tiene grandes limitaciones en cuanto al uso de múltiples interfaces de red (y hay que notar el hecho de que dispositivos IoT tales como pasarelas inteligentes de red y teléfonos inteligentes tienen típicamente diferentes interfaces). Esto obviamente tiene importantes consecuencias a la hora de aprovechar el ancho de banda, posibilidades sobre el uso de varios canales disponibles, durabilidad de la conexión, y también, de manera importante, con el gasto energético de la transmisión. A pesar de las limitaciones de TCP, originalmente pensado para conexiones cableadas y no para la IoT, muchos expertos consideran que para que el ecosistema IoT funcione, soporte aplicaciones y sea capaz de acomodar la gran heterogeneidad de dispositivos inteligentes y tipos de aplicaciones sobre ella, la IoT debe adoptar el uso del protocolo TCP/IP y sus estándares abiertos [20][89].

El reciente protocolo Multipath TCP o MPTCP [90](una extensión de TCP considerada como un protocolo de transporte propio) permite la interoperabilidad de caminos de transmisión de datos en conexiones TCP, el alivio global y un uso inteligente y

eficiente de los recursos de red (multiplicando la eficiencia actual), una mayor eficiencia energética en la transmisión de datos y la interoperabilidad de interfaces de red dentro de un mismo host (interoperabilidad técnica). Estos temas están muy relacionados con la interoperabilidad técnica y la eficiencia energética. Además, MPTCP está estrechamente relacionado con un probable pilar arquitectónico del Internet del Futuro: el principio de reparto global de los recursos [91][92]. MPTCP tiene características que ayudan notablemente a un mejor reparto de recursos de la red entre las distintas conexiones. Otra tendencia creciente en las redes es el acelerado y vertiginoso aumento de dispositivos IoT móviles como tabletas y teléfonos inteligentes, en los cuales el uso de MPTCP aporta grandes ventajas. Por todas estas razones, MPTCP se ve como una pieza de gran importancia en el internet del futuro.

Desde el punto de vista de la interoperabilidad hay que notar que como protocolo de transporte MPTCP es un habilitador de la interoperabilidad técnica para la comunicación de elementos conectados a través de la red (ej. dispositivos y plataformas IoT). Es muy destacable que, por sus características especiales, el protocolo MPTCP y un control de congestión eficiente asociado potencialmente pueden permitir un uso más eficiente de las redes, y con ello mejorar el nivel de interoperabilidad técnica que estas proporcionan.

En el recorrido de esta tesis doctoral se ha estudiado el uso del protocolo MPTCP, formas de control de congestión inteligente por estudio de tiempos, y se ha diseñado e implementado un nuevo algoritmo de MPTCP para mejorar el control de congestión de conexiones Multipath, aliviar de manera muy significativa la congestión en redes (no solo de la propia conexión) y permitir un uso mucho más eficiente de los recursos de transporte de la red. En última instancia, esta eficiencia permitiendo el uso y aprovechamiento de múltiples interfaces de red entre los equipos o entidades que realizan la conexión. Este algoritmo es muy novedosos ya que permite tener las ventajas de los algoritmos basados en una detección y control inteligente de la congestión por medida de tiempos, sin ninguna de sus grandes vulnerabilidades y debilidades (incompatibilidad para funcionar con el tipo de tráfico mayoritario en internet, que utiliza estrategias de control de congestión más primitivas e ineficaces), y por tanto, ofreciendo ventajas que no posee ningún otro algoritmo de congestión.

3.2. Nueva extensión de TCP: Multipath TCP

3.2.1. TCP

El Protocolo de Control de Transmisión (TCP) [1] es el protocolo de transporte más utilizado en Internet, el cual proporciona una entrega segura de un flujo de datos entre los dos puntos o host finales. Es decir, TCP debe proporcionar y garantizar un flujo seguro y ordenado de bytes libres de errores desde el emisor hasta el receptor. Las principales aplicaciones de Internet dependen de TCP, siendo responsables de más del 85% del tráfico en Internet [93].

TCP se encuentra en el nivel intermedio entre el protocolo de Internet (IP) y el protocolo de aplicación. Normalmente, las aplicaciones requieren una comunicación fiable, lo que significa que los bytes enviados de una aplicación a otra deben ser idénticos a los recibidos, sin errores y en el mismo orden. El servicio de datagramas de la capa IP no puede garantizar la fiabilidad de los datos, pero TCP proporciona la funcionalidad necesaria para permitir una comunicación segura y fiable entre dos puntos finales.

El flujo de datos a transmitir se divide en paquetes numerados de bytes, que se encapsulan en segmentos TCP y se envían al receptor. Cada segmento tiene un número de secuencia que permite reconstruir el flujo de datos en el orden correcto en el otro punto final. TCP requiere la confirmación del mensaje para garantizar la fiabilidad de los datos. Cada paquete recibido correctamente se confirma enviando un mensaje ACK en respuesta al remitente. En caso de que no se reciba un acuse de recibo después de un tiempo razonable, el emisor TCP retransmitirá el paquete aparentemente perdido.

Aparte de la transmisión segura de datos, el control de congestión de extremo a extremo es otra función principal de TCP, y será explicado en detalle en la sección 1.3 ya que tiene especial relevancia en este capítulo. No solo los datos deben llegar a su destino, también el flujo entre los dos hosts debe ser regulado adecuadamente para evitar en la medida de lo posible situaciones de congestión de red.

3.2.2. MPTCP

Multipath TCP [94][95][96] es una reciente extensión del protocolo TCP [97] que permite que las conexiones TCP puedan utilizar simultáneamente varios caminos a través de la red para una misma transmisión de datos. Es decir, permite que una conexión de datos se extienda a través de múltiples caminos en la red, y que los datos a enviar se distribuyan entre los distintos caminos establecidos. Esta es una nueva y revolucionaria posibilidad no factible anteriormente con el protocolo TCP clásico, el cual limita el enrutado de datos a un único camino en la red y a una sola interfaz de red del host transmisor.

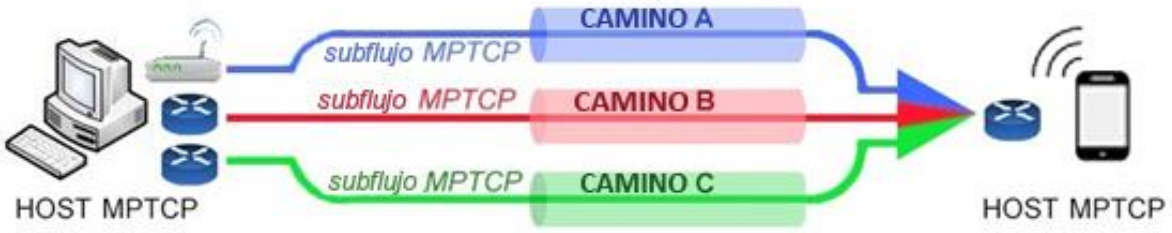


Figura 3.1 Ejemplo de una conexión MPTCP compuesta por 3 subflujos de datos.

El uso de múltiples caminos para una sola transmisión de datos es posible utilizando diferentes conexiones TCP simultáneamente entre los dos hosts finales, que actúan conjuntamente como una sola para la capa de aplicación, ya que se transmite solo un único flujo de datos a través de todo el conjunto.

Es posible establecer varias subconexiones TCP si al menos uno de los puntos finales presenta múltiples interfaces de red y cada interfaz de red recibe una dirección IP diferente (práctica de multihoming o multiconexión). MPTCP permite establecer una subconexión TCP adicional para cada interfaz extra de cualquiera de los hosts finales. Esos flujos TCP individuales se denominan "subflujos" de la conexión MPTCP a la que pertenecen, y suelen enrutarse a través de diferentes caminos a través de la red, que se suponen disjuntos o parcialmente disjuntos. La carga se distribuye entre esos subflujos.

MPTCP amplía la capa de transporte con una funcionalidad adicional sobre TCP. En la capa inferior, una conexión MPTCP aparece como múltiples conexiones TCP

(subflujos), mientras que la capa superior mantiene sólo una conexión. MPTCP amplía TCP utilizando algunos campos de cabecera opcionales [92].

Durante el modo handshake de la conexión TCP, los hosts finales pueden negociar el uso de MPTCP. Los hosts pueden entonces intercambiar las diferentes direcciones IP de las interfaces de red adicionales y decidir la adición de más subflujos o subconexiones. Más adelante, tras la fase handshake, será posible añadir más subflujos o eliminar los anteriores.

3.2.3. Ventajas frente a TCP

El uso de TCP de un único camino en la red implica que el rendimiento de la conexión está completamente restringido a las limitaciones del camino (capacidad de carga y su situación de congestión) y no se pueden obtener los beneficios del uso de múltiples interfaces de red.

En contraste, la utilización de múltiples caminos permite eludir estas limitaciones y la dependencia de la situación del camino. Este nuevo enfoque permite mejorar dramáticamente el rendimiento, la solidez y la fiabilidad de la conexión. La conexión se vuelve resistente a los problemas de un trayecto -se mantiene incluso en caso de fallo persistente del enlace- y la fiabilidad mejora muy significativamente gracias a esta mayor robustez. El rendimiento de la conexión no se ve limitado por el ancho de banda y el nivel de ocupación de una sola ruta, ya que es posible agrupar la capacidad en todas las rutas disponibles. Destaca entre sus grandes ventajas la flexibilidad para adaptarse a la situación de la red y los caminos, la posibilidad de uso de varias interfaces de red (situación común en pasarelas IoT de redes y en dispositivos IoT tales como teléfonos móviles) y la muy notable habilidad para mejorar la situación de congestión no solo de la propia conexión debido a esta flexibilidad, sino indirectamente de manera global en la red. También permite el uso de mayor ancho de banda que una conexión TCP convencional.

Esto es posible mediante el uso de múltiples conexiones TCP entre los dos hosts finales, que funcionan conjuntamente como una sola extremo a extremo para la capa de aplicación -la conexión MPTCP-, ya que sólo se transmite un único flujo de datos a través de todo el conjunto. Esto es posible aprovechando el uso del conjunto de interfaces de red (multihoming): por cada interfaz de red adicional en cualquiera de

los hosts finales, MPTCP permite establecer una conexión TCP adicional. Los datos que se envían se distribuyen entre esas subconexiones, que normalmente se enrutan a través de diferentes caminos en la red.

MPTCP se creó bajo el principio de agrupación de recursos [98], un nuevo principio arquitectónico propuesto para guiar el desarrollo de Internet del Futuro. El concepto de agrupación de recursos significa hacer que un conjunto de recursos de red se comporte como un solo recurso en conjunto. El método para conseguir una agrupación de recursos y un mejor reparto global de estos consiste en crear mecanismos para desplazar la carga entre las distintas partes de la red.

La propuesta para conseguir un mecanismo nuevo, sencillo, flexible y potente para la puesta en común de recursos consiste en aprovechar la capacidad de respuesta de los sistemas finales de la forma más genérica posible: acoplando el control de la congestión con el enrutamiento multitrayecto. La responsabilidad de esta acción se otorga a los sistemas finales para que puedan actuar de forma global.

Si los sistemas finales distribuyen su carga a través de múltiples caminos de forma correcta, reaccionando adecuadamente a las señales de congestión de la red, entonces el tráfico se alejaría rápidamente de los enlaces congestionados o fallidos en favor de los enlaces no congestionados. Esta forma de agrupación de recursos no sólo aumenta la fiabilidad, la flexibilidad y la eficiencia, sino que también proporciona un enrutamiento consciente de la congestión y carga de tráfico.

3.3. Control de la congestión

El control de la congestión extremo a extremo es una de las funciones principales del protocolo TCP. Los hosts finales de cualquier conexión TCP se encargan de regular adecuadamente su flujo de datos intentando evitar congestión en la red. Un tráfico superior a lo que la red puede soportar provoca un desbordamiento de los recursos de la red, pérdidas de paquetes, la consiguiente necesidad de retransmisiones, retrasos y una grave degradación de la calidad del servicio de la red. Si el sistema no puede salir de este estado y los niveles de tráfico siguen siendo excesivos, puede producirse un colapso por congestión, lo que lleva a un funcionamiento caótico de la red que hace imposible una comunicación efectiva [99][100].

MPTCP ofrece nuevas y revolucionarias capacidades para el control de la congestión imposibles anteriormente con TCP clásico de un solo camino. TCP sólo puede adaptar su rendimiento a la situación de congestión de la ruta seleccionada por el sistema de enrutamiento. En caso de que la conexión se enrute por enlaces sobreutilizados, TCP sólo puede reducir la tasa de transmisión para intentar evitar el colapso de la red.

Sin embargo MPTCP puede desviar el tráfico de las rutas más congestionadas a las menos utilizadas. Esto no sólo beneficia al rendimiento de la conexión, sino que también mejora indirectamente el rendimiento de la red, ya que MPTCP alivia los enlaces congestionados, lo que conduce a una mejor distribución del tráfico y a una asignación más justa de los recursos de red. En lugar de limitarse a adaptarse a la congestión, MPTCP puede resolver los problemas de congestión desplazando el tráfico de los enlaces sobrecargados a los menos utilizados.

Por esta capacidad de reajuste de tráfico en la red, el uso de MPTCP se considera la mejor y única forma eficaz de resolver el actual problema de congestión en Internet, más allá de intentar aumentar la capacidad de las redes. Hay que tener en cuenta que los sistemas de enrutamiento no disponen de la inconmensurable cantidad de información global que sería necesaria para conseguir un rendimiento óptimo de la red.

Además, la capacidad de MPTCP de agrupar ancho de banda de distintos caminos permite una flexibilidad muy útil para manejar la asignación de recursos. Permitir que los puntos finales tomen algunas decisiones de enrutamiento, y que tengan varias opciones de enrutamiento, parece ser la clave para lograr un enrutamiento más eficiente, que conduzca a una asignación de recursos más optimizada y a la obtención de un rendimiento de red superior. La técnica habitual para la prevención de congestión siempre ha sido actuando individualmente sobre puntos específicos sobrecargados, pero actualmente empiezan a hacerse evidentes los beneficios de prevenir la congestión mediante un enfoque más global [101].

Todas estas interesantes ventajas sólo pueden obtenerse equilibrando adecuadamente el tráfico en los caminos disponibles, lo cual es una nueva tarea añadida para el algoritmo de control de la congestión. Los algoritmos de congestión clásicos para TCP no tienen esa función al haberse diseñado considerando un único camino y por ello deben diseñarse nuevos algoritmos para MPTCP. Los detalles del

diseño tienen una importancia crucial para el rendimiento de la conexión, que depende en gran medida del control de la congestión.

Los algoritmos de control de congestión existentes para MPTCP, mencionados en las secciones 3.3.3 y 3.4, son pocos y están basados principalmente en algoritmos de generación de pérdidas, en los que es inherente la generación de cierto grado congestión y pérdida de eficiencia por pérdidas de paquetes. Solo wVegas [102] explora el uso de un sistema eficiente de control de congestión, y con la excepción del nuevo algoritmo creado en el marco de esta tesis doctoral, no existe ningún algoritmo híbrido de control de congestión de alta eficiencia para MPTCP.

El control de congestión tradicional para el protocolo TCP se basa en las pérdidas: la congestión se detecta sólo cuando ya está provocando pérdidas de paquetes, lo que tiene un coste elevado en cuanto a la conexión y el rendimiento de la red. Además, el control de la congestión basado en las pérdidas requiere provocarlas periódicamente para determinar el límite del ancho de banda disponible; paradójicamente, esto hace que la congestión sea algo inherente a este tipo de control de la congestión.

Por otro lado, existe un enfoque diferente para el control de la congestión, alternativo al basado en pérdidas y mucho más eficiente. Este enfoque puede detectar la congestión incipiente antes de que se produzca la pérdida de paquetes mediante un análisis inteligente de la información de retardo de los paquetes de datos. Los algoritmos basados en el retardo son capaces de prevenir la congestión, en lugar de limitarse a reaccionar ante ella, lo que conduce a un mayor y más eficiente rendimiento de la conexión y de la red.

El control de la congestión MPTCP actual podría mejorarse mediante la creación de nuevos y más eficaces algoritmos de control de congestión. MPTCP tiene un número significativamente menor de algoritmos de congestión que TCP debido a su reciente creación y a la complejidad adicional que implica garantizar el control de congestión entre múltiples caminos –estos algoritmos tienen un diseño significativamente más complejo que los algoritmos para TCP de un solo camino- (LIA [103], OLIA [91], BALIA [104], wVegas [105] y Cubic [106]).

La capacidad de prevenir la congestión de forma más eficiente, evitando así las pérdidas de paquetes, muy costosas para el rendimiento de la red, conduciría a un

mejor servicio de enlace y también mejoraría el rendimiento de la conexión. El análisis de retrasos también puede proporcionar información precisa sobre el ancho de banda disponible en los trayectos, lo que podría ayudar a conseguir una asignación de recursos y una distribución del tráfico más eficientes y justas. El rendimiento de la red también se beneficiaría de ello. Además, el diseño de un algoritmo de control de la congestión por retardo para MPTCP podría llevarse a cabo sorteando graves problemas y deficiencias que afectan a Reno, el algoritmo estándar de TCP, y a algoritmos basados en Reno y en el control de congestión por pérdidas.

Las redes de alta velocidad están alcanzando una gran importancia en Internet, y se necesitan sustitutos de Reno -capaces de actuar eficientemente en esas redes, a diferencia de Reno. Por desgracia, el otro tipo de algoritmos de control de congestión, basados en análisis de tiempos, a pesar de su gran eficiencia en comparación con los basados en pérdidas, no son capaces de proporcionar una transmisión efectiva cuando comparten canal con tráfico que utiliza control de congestión por pérdidas, el cual es el tipo de tráfico habitual en las redes. Este es el caso de wVegas, el único algoritmo de control de congestión basado en retardo en MPTCP.

Por ello, el diseño de un nuevo algoritmo basado en el retardo para MPTCP capaz de funcionar con un rendimiento adecuado ante tráfico basado en pérdidas, y a la vez proporcionar un control de congestión inteligente y altamente eficiente, explotaría las notables posibilidades del control de la congestión por retardo en MPTCP, y a la vez aportaría grandes mejoras al tipo de control de congestión por análisis inteligente de retardo.

En esta tesis doctoral se ha diseñado el primer algoritmo de congestión híbrido para MPTCP (que combina técnicas de análisis de tiempo con técnicas de resistencia de algoritmos basados en pérdidas), creando una nueva familia de algoritmos de control de congestión en MPTCP. Además, como trabajo preludio al desarrollado en la tesis doctoral, se ha hecho un estudio [101] sobre algoritmos de congestión, presentado al IETF una propuesta del primer algoritmo basado en análisis de tiempos para MPTCP [107] de manera simultánea al actualmente conocido como wVegas [105], además de un análisis alternativo del principal algoritmo de control de congestión de MPTCP, LIA, basado en Reno en su periodo de estandarización, y las técnicas de control de congestión basadas en pérdidas [92].

3.3.1. Requisitos específicos del control de congestión multicaminos

El control de congestión en TCP de múltiples caminos (MPTCP) tiene una nueva responsabilidad frente al TCP convencional: la gestión eficiente de la carga y la congestión entre los distintos caminos. Esto hace su diseño y ejecución considerablemente más complejos. Hay que notar también, por otra parte, que como objetivos de diseño en el control de congestión de MPTCP, establecidos por parte de los creadores de este nuevo protocolo, se exige que además de un reparto multicaminos del flujo de datos, se haga un uso no abusivo del ancho de banda disponible para no dejar en desventaja al tráfico TCP clásico, aun presentando cierta mejora frente a TCP, y por otro lado equilibrar la utilización y congestión en los caminos en la medida de lo posible. Estos objetivos están detallados en la sección 3.4.1.1.

3.3.2. Conceptos clave de control de congestión

Para poder entender el funcionamiento de un algoritmo de congestión, se ha considerado necesario introducir los siguientes conceptos [108]:

Ventana de congestión

Para regular la transmisión de paquetes, TCP utiliza un control de flujo basado en ventanas. Cada fuente mantiene una variable de "tamaño de ventana" que limita el número máximo de paquetes que pueden estar pendientes (en vuelo): se transmite al receptor pero aún no se ha recibido un mensaje de confirmación de su recepción o ACK. Cuando una ventana de datos está pendiente, la fuente debe esperar un acuse de recibo antes de enviar un nuevo paquete. Esta variable del tamaño de la ventana, denominada ventana de congestión (CWND), determina la velocidad de la fuente: se envía aproximadamente el valor de una ventana de paquetes cada tiempo de ida y vuelta (RTT), es decir, el tiempo que tarda el emisor en recibir la confirmación de un paquete enviado (ACK). El TCP estándar aumenta la CWND de forma aditiva a medida que se reciben paquetes en aproximadamente un paquete por RTT, y disminuye la ventana de forma multiplicativa cuando se detecta congestión. De esta manera se regula la tasa de transmisión de paquetes. Esta estrategia se denomina AIMD

(Additively Increase, Multiplicative Decrease). Con este sistema de ventanas, TCP puede reducir automáticamente la velocidad de la fuente cuando la red se congestiona y los ACKs se retrasan: tras señales explícitas de congestión (pérdida de paquetes) TCP disminuye bruscamente la velocidad de envío.

Eventos de pérdida

El emisor TCP retransmite cualquier paquete perdido para garantizar la fiabilidad de los datos. La pérdida de paquetes es una señal de congestión. Este evento tiene dos categorías diferentes: la pérdida detectada por ACKs duplicados (evento de pérdida normal) y la pérdida detectada por tiempo de espera agotado (evento de Timeout).

Cada paquete de datos enviado inicia un temporizador de retransmisión en el emisor TCP. Si hay un tiempo de espera y aún no ha llegado el acuse de recibo del mensaje, el paquete se retransmite y el CWND se restablece al tamaño máximo del segmento (MSS).

Si se recibe un paquete cuando se espera otro anterior, el receptor TCP envía un ACK duplicado como respuesta confirmando la recepción pero también informando de que falta el paquete con el número de secuencia esperado. Tres ACK duplicados reclamando el mismo paquete provocan su retransmisión. Entonces el CWND suele reducirse a la mitad -dependiendo de la implementación de TCP que utilice el transmisor-.

En consecuencia, la tasa de transmisión se reduce considerablemente para mitigar la congestión, pero no tan drásticamente como en el caso de un tiempo de espera, dado que no se espera que la congestión sea crítica, ya que los ACKs siguen llegando.

Estructura de las fases TCP para el control de la congestión o algoritmo genérico

Las implementaciones modernas de TCP contienen cuatro algoritmos o fases entrelazadas para el control de la congestión: inicio lento, evitar la congestión, retransmisión rápida y recuperación rápida. Estos cuatro algoritmos componen un algoritmo completo de control de la congestión, y todos los algoritmos de

control de congestión para TCP o MPTCP actuales son particularizaciones de este conjunto de cuatro métodos o fases.

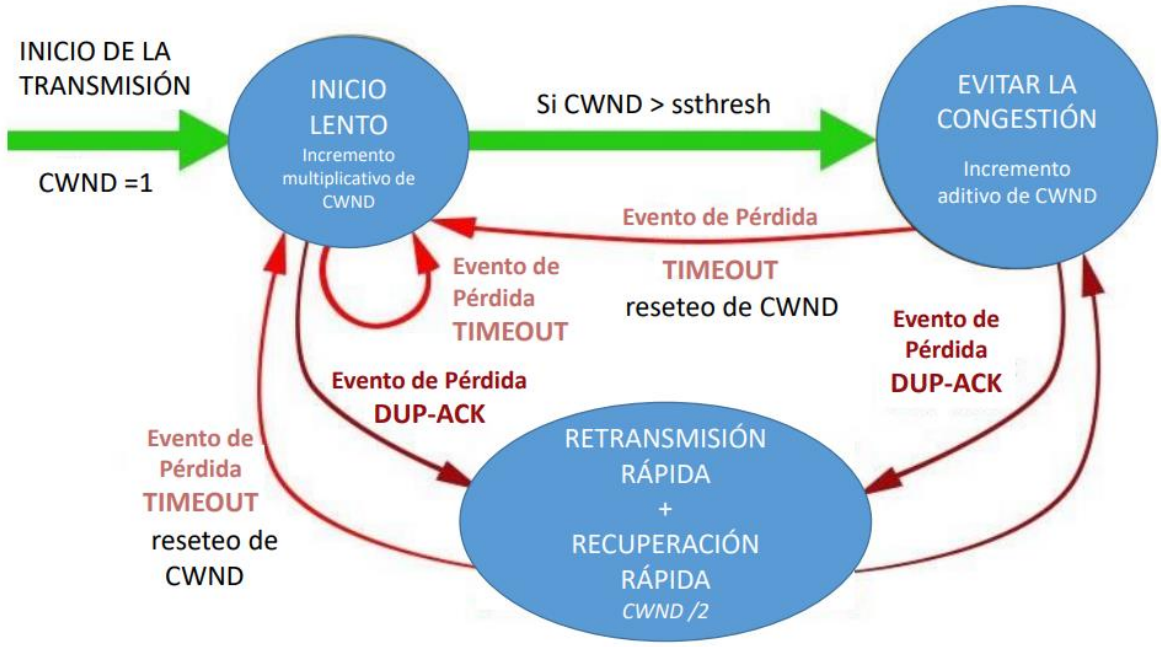


Figura 3.2 Diagrama de las fases y estados de la transmisión.

El inicio lento y la fase evitar la congestión son los responsables del aumento del CWND. El inicio lento se utiliza al principio de la transmisión para permitir un incremento rápido para luego entrar en el modo de evitación de la congestión. En caso de pérdida, la transmisión sale temporalmente de cualquiera de esos estados. Si la pérdida es detectada por un tiempo de espera después de la retransmisión del paquete y el reinicio de CWND la transmisión entra en la fase de inicio lento. En caso de detección de pérdida por ACKs duplicados, los algoritmos de retransmisión rápida y recuperación rápida gobiernan temporalmente la transmisión, para luego pasar al modo de evitación de congestión.

El comportamiento general de estos algoritmos o fases se explica en detalle a continuación, aunque puede variar para cada implementación de TCP.

Inicio lento

El emisor TCP utiliza el algoritmo de inicio lento cuando el tamaño de la ventana de congestión está por debajo del umbral SSTHRESH. Esto ocurre al principio de la transmisión cuando el CWND comienza con un valor muy pequeño, dos veces el tamaño máximo del segmento (MSS), y después de un tiempo de espera, cuando el CWND se restablece. En estas situaciones el CWND es mínimo y se desconocen las condiciones actuales de la red, lo que hace conveniente un incremento rápido para explorar rápidamente el ancho de banda disponible. La tasa de incremento es multiplicativa: por cada paquete reconocido, la ventana de congestión se incrementa en 1 MSS, duplicando por tanto su valor por cada tiempo de ida y vuelta (RTT). Un aumento aditivo que comience con una CWND muy pequeña podría tardar demasiado en utilizar una parte normal del ancho de banda disponible.

El valor inicial de SSTHRESH suele ser grande. Este umbral se actualiza al final de cada inicio lento. Hasta que se obtiene un valor adecuado según las condiciones de la red, el inicio lento suele terminar tras un tiempo de espera, ya que la tasa de transmisión con crecimiento multiplicativo supera rápidamente la capacidad de la red. Cuando la ventana de congestión supera el umbral SSTHRESH, la transmisión pasa del modo de arranque lento al de evitación de la congestión y adopta un crecimiento menos agresivo.

Evitar la congestión

El emisor TCP utiliza la evitación de la congestión cuando el CWND está por encima del umbral SSTHRESH. En un funcionamiento normal, este es el estado que rige principalmente la transmisión. Los diferentes esquemas de control de la congestión para TCP difieren principalmente en el diseño de este algoritmo.

La ventana de congestión presenta un incremento menos agresivo que en la fase de inicio lento -aditivo en lugar de multiplicativo por RTT-. Este crecimiento es más apropiado cuando la tasa de transmisión se ajusta aproximadamente a la capacidad de la red, condición necesaria para salir de la fase de inicio lento. Para la implementación estándar de TCP el incremento de CWND es aproximadamente de un paquete (1 MSS) por RTT.

Retransmisión rápida y recuperación rápida

Cuando un paquete llega fuera de orden al receptor -con un número de secuencia más alto que el siguiente paquete esperado- se envía un ACK duplicado en respuesta confirmando esta recepción pero también informando de que falta el paquete esperado.

Después de tres ACKs duplicados, el paquete se considera perdido y se retransmite. Este procedimiento se denomina retransmisión rápida, ya que el mensaje se vuelve a enviar sin esperar a que se agote el tiempo de espera.

Mientras el ACK del paquete retransmitido no haya llegado, la transmisión se rige por el modo de recuperación rápida. SSTRESH se ajusta a CWND/2. Los nuevos paquetes se transmiten mientras el CWND y la ventana de recepción lo permiten. Por cada ACK duplicado que llega en este estado CWND se incrementa en 1 MSS. Cuando llega el ACK esperado, CWND se establece en SSTRESH (el CWND anterior a la fase de recuperación rápida se reduce a la mitad) y la transmisión entra en el modo de evitar la congestión.

3.3.3. Tipos de control de congestión

3.3.3.1 *Control de Congestión basado en Pérdidas*

Este tipo de control de congestión es el más utilizado en Internet. Los esquemas tradicionales de control de la congestión para TCP se basan en las pérdidas, ya que la pérdida de paquetes es el único indicativo de congestión que saben detectar. Eso significa que sólo son capaces de detectar la congestión cuando ya está causando pérdidas y, por lo tanto, ya se ha dañado el rendimiento de la conexión y se ha congestionado el enlace [109].

La única forma que tienen los algoritmos basados en pérdidas para comprobar el ancho de banda disponible en el enlace (para no infrautilizar esta capacidad) es aumentar su rendimiento hasta superar el límite del ancho de banda disponible y provocar la pérdida de paquetes y una situación de congestión. Por ello, las pérdidas son intrínsecas y periódicas en este tipo de control de la congestión.

Su mecanismo para controlar la congestión presenta un aumento gradual del CWND hasta que se produce un evento de pérdida. Tras detectar las pérdidas, la tasa se

reduce bruscamente para seguir aumentando gradualmente de nuevo, siguiendo la estrategia AIMD para el crecimiento del CWND ("Additive Increase, Multiplicative Decrease").

Este tipo de control de la congestión es incapaz de evitar la pérdida de paquetes, la cual es necesaria e inherente a él, ya que debe provocarse periódicamente para conocer el límite del ancho de banda disponible. El mejor ejemplo de su implementación en TCP es TCP Reno, el algoritmo más usado en Internet y que presenta muchísimas variantes. En MPTCP, el algoritmo equivalente a TCP Reno (en el que está basado) es LIA. LIA es básicamente una adaptación multicaminos de Reno con cierta funcionalidad adicional requerida para MPTCP [103]. A continuación se describen y analizan ambos algoritmos.

<u>Control de congestión basado en pérdidas en TCP: Reno</u>

La implementación estándar de TCP (TCP Reno) [110] se basa en las pérdidas, siguiendo el esquema AIMD con el factor de aumento $\alpha = 1$ y el factor de disminución $\beta = 1/2$.

El algoritmo para evitar la congestión aumenta el CWND en 1/CWND por cada ACK recibido, lo que significa un incremento aditivo de 1 segmento por RTT. Cada vez que se detecta un evento de pérdida normal, CWND se reduce a la mitad -teniendo también una retransmisión rápida y una entrada temporal en la fase de recuperación rápida-. En caso de pérdida de tiempo, el CWND se reinicia.

Algoritmo 3.1: Reglas de aumento y disminución de CWND de TCP Reno.

Incremento	$CWND \rightarrow CWND + 1/CWND$ **por ACK** $= \boldsymbol{CWND} + 1MSS$ **por RTT**	(1)
Disminución	$CWND \rightarrow CWND/2$ por **pérdida con ACK duplicado**	(2)
Expiración de tiempo de espera	$CWND \rightarrow CWND$ inicial	(3)

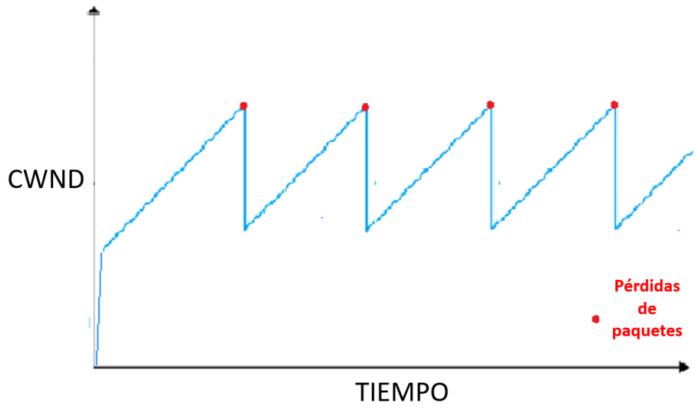


Figura 3.3 Comportamiento de Reno en un enlace dedicado, no compartido con otras conexiones. Hay pérdidas al alcanzar la capacidad máxima disponible en el enlace y consiguiente pérdida de rendimiento.

Hay que tener en cuenta que TCP Reno presenta algunos problemas importantes que en general heredan los algoritmos de control basado en pérdidas (los cuales se pueden considerar modificaciones de TCP Reno):

- ***Rendimiento deficiente en redes de alta velocidad: el*** rendimiento de Reno en enlaces con un gran producto de ancho de banda y retardo (BDP) es deficiente, ya que la función de incremento lineal puede tardar mucho tiempo en alcanzar la plena utilización de un enlace tras un evento de congestión, lo que no permite utilizar eficazmente el ancho de banda.
- ***Desigualdad de RTT*** - Los flujos Reno con mayor RTT son menos agresivos compitiendo por el ancho de banda disponible que los flujos Reno con menor RTT, y consiguen una cuota menor.
- ***Convergencia lenta*** - Cada vez que se pone en marcha un flujo adicional, la convergencia al estado estacionario lleva mucho tiempo.
- ***Sensibilidad a la provisión de búfer*** - El rendimiento de Reno es sensible a la cantidad de búfer en el enlace cuello de botella. El tamaño óptimo del buffer para una conexión Reno es el producto ancho de banda-retraso (BDP). Si la cola es demasiado corta para una ruta determinada, el

rendimiento se verá afectado. Si es demasiado larga, la latencia de la red será alta, ya que Reno mantendrá una cola de espera.

Control de congestión basado en pérdidas en MPTCP: LIA

Linked Increased Algorithm (LIA) [91][92] está basado en Reno, adaptado para MPTCP incorporando la función de gestión de múltiples caminos.

Como se puede observar, este algoritmo es significativamente más complejo que Reno debido a la complejidad añadida de la gestión multicamino. El aumento de CWND por ACK es el mismo para todos los subflujos, ya que está acoplada por el factorα/W total, común a todos ellos. Es decir, el factor de crecimiento está interrelacionado con todos los subflujos, depende de todos ellos y es igual para todos ellos. Por el contrario, la disminución sigue la regla de disminución de Reno y, en consecuencia, es completamente independiente del rendimiento de los otros subflujos. El factor α que ajusta la agresividad del incremento depende de los parámetros de todos los subflujos (tasa, CWND, RTT) y se ha obtenido derivando las ecuaciones de equilibrio de Reno mientras se exige el cumplimiento de los objetivos de diseño de MPTCP.

Algoritmo 3.2: Reglas de aumento y disminución de CWND de MPTCP LIA.

$$\text{Aumentar} \quad W_i \text{ por } \min\left(\frac{\alpha}{W_{total}}, \frac{1}{W_i}\right) \quad \text{Por ACK en el subflujo i} \tag{4}$$

$$\text{Disminuir} W_{total} \text{ a } \max\left(\frac{W}{2}, 1\right) \quad \text{Por evento de pérdida normal} \tag{5}$$

$$W_i = CWND \text{ del subflujo en el trayecto i} \tag{6}$$

$$W_{total} = \sum W_i \tag{7}$$

$$\alpha = W_{total} \frac{\max\left(\frac{W_i}{RTT_i^2}\right)}{\left(\sum \frac{W_i}{RTT_i}\right)} \tag{8}$$

El algoritmo utiliza un comportamiento TCP no modificado en caso de caída -confía en los mecanismos TCP tradicionales para detectar caídas, retransmitir datos, etc.

Actualmente, los únicos algoritmos existentes para el control de congestión de MPTCP (LIA BALIA OLIA semicoupled wVegas) están basados en Reno con la excepción de wVegas. Desgraciadamente, estos algoritmos de control de congestión basados en pérdidas presentan algunas graves deficiencias heredadas de Reno, como la muy baja eficacia y rendimiento en redes de alta velocidad.

Se puede encontrar más información sobre el funcionamiento de LIA en [91][92]. En concreto [92] fue una implementación y análisis de LIA en un sistema operativo real hecho por la autora de esta tesis en la fase de estandarización de este protocolo. Este trabajo sentó las bases para el desarrollo de un nuevo algoritmo de congestión de MPTCP en el marco de esta tesis, ya que permite conocer las debilidades y aspectos de mejora del control de congestión basado en pérdidas en MPTCP.

Los algoritmos actuales de control de congestión para MPTCP están basados en Reno y LIA, con la excepción de wVegas: LIA [92], OLIA [91], BALIA [104], Cubic [111] e inclusive el fallido Fully Coupled [112], el cual no se considera un algoritmo adecuado

para el uso actual en la red. Por tanto, el control de congestión de MPTCP está actualmente mayormente basado en pérdidas. OLIA, BALIA y Cubic son una evolución de LIA en la que se mejoran ciertos aspectos negativos de este último algoritmo.

3.3.3.2 *Control de Congestión basado en Análisis de Tiempos*

El control de la congestión basado en el retardo detecta la congestión en una fase incipiente -antes de causar la pérdida de paquetes, observando el aumento de los valores de RTT, ya que el retardo de las colas aumenta mucho cuando los enrutadores de red se empiezan a sobrecargar. Esta detección temprana permite una acción proactiva contra la congestión, reduciendo adecuadamente la tasa de transmisión para evitar que la cola del enlace se llene por completo y, por tanto, la pérdida de paquetes. En contraste, el control de la congestión basado en pérdidas sólo puede ser reactivo ante la presencia de pérdidas, teniendo un rendimiento inferior y mucho menos eficiente debido al elevado coste de las pérdidas de paquetes en el rendimiento.

Además, el análisis de los retrasos proporciona una información más completa sobre las condiciones de la red que la que pueden aportar los eventos de pérdidas. Los esquemas basados en pérdidas son incapaces de estimar la capacidad disponible, por lo que requieren aumentar constantemente su caudal entre disminuciones multiplicativas para no infrautilizar esta capacidad, hasta superar inevitablemente su límite y provocar una congestión. Por el contrario, los esquemas basados en el retardo buscan ajustar y mantener su tasa de transmisión en el rango de valores estimados como óptimos, presentando un rendimiento más suave y eficiente que el comportamiento oscilante de los esquemas basados en pérdidas.

Una capacidad clave en la eficacia del análisis de los retrasos es la estimación precisa del retraso actual de las colas o buffers – es decir, el tiempo que un mensaje y su ACK llevan almacenados en las colas de los enrutadores de red a la espera de ser procesados-. Se requiere una medición precisa de los tiempos, pero también una buena estimación del retardo de propagación, el tiempo que tarda un mensaje en cruzar la red hasta su destino más su ACK en volver cuando no hay congestión. El valor del tiempo de ida y vuelta es la suma de ambos retrasos.

Este tipo de control de la congestión conduce a un rendimiento mejor, más justo y más eficiente que el control de la congestión tradicional basado en las pérdidas. La congestión, las pérdidas y las posteriores retransmisiones se evitan en su mayor parte, ahorrando su costoso coste en rendimiento. Además, los esquemas basados en el retardo proporcionan equidad en el RTT, y también funcionan eficazmente en redes de alta velocidad cuando ese rendimiento no se ve afectado por la presencia de tráfico cruzado basado en pérdidas.

Actualmente, los únicos algoritmos existentes para el control de congestión de MPTCP (LIA[] BALIA[], OLIA[], Cubic [] y wVegas[]) están basados en Reno con la excepción de wVegas. Desgraciadamente, estos algoritmos de control de congestión basados en pérdidas presentan algunas graves deficiencias heredadas de Reno, como la ineficacia cuando se trata de redes de alta velocidad [].

Control de contestión basado en el retraso para TCP: Vegas

Vegas [100] es un algoritmo de control de la congestión basado en el retardo para TCP que consigue entre un 40% y un 70% más de rendimiento y entre una quinta y la mitad de pérdidas que Reno, el algoritmo estándar de control de la congestión de TCP, en condiciones de red y congestión normales. Esta estado de red dentro de la normalidad se entiende mientras las memorias o buffers intermedios de la red son capaces de mantener los paquetes pendientes, es decir sin episodios de congestión grave o colapso de red.

Vegas es capaz de interoperar con cualquier otra implementación válida de TCP, pero el rendimiento de la conexión se degrada mucho al compartir enlaces con conexiones cuyo control de congestión está basado en pérdidas (CCP) [109].

Para mejorar el control de congestión TCP, Vegas emplea nuevos mecanismos: una estrategia de cálculo para controlar la congestión evitando la pérdida de paquetes y la sobrecarga de bufferes de la red, un algoritmo de inicio lento amortiguado y algunos cambios que afectan a la estrategia de retransmisión de TCP.

El esquema del algoritmo Vegas puede verse en el esquema 3.3.

Algoritmo 3.3: Reglas de aumento y disminución de CWND de Vegas

$$W \rightarrow \begin{cases} W+1 & diff < \alpha \\ W & \alpha < diff < \beta \\ W-1 & diff > \beta \end{cases} \quad \text{Comprobado cada RTT} \tag{9}$$

$$W \rightarrow W - \frac{W}{4} \quad \text{por dup-pérdida de ACK} \tag{10}$$

W se restablece en caso de que se agote el tiempo de espera

$$diff = \text{Tasa esperada} - \text{Tasa real} \tag{11}$$

$$\text{Tasa real} = \frac{W}{RTT} \tag{12}$$

$$\text{Tasa esperada} = \frac{W}{BaseRTT} \tag{13}$$

$$BaseRTT = \text{retardo de propagación estimado} \tag{14}$$

La *tasa esperada* es el rendimiento que podría alcanzarse en caso de ausencia de congestión en la red. Esta tasa de transmisión máxima se estima dividiendo el tamaño de la ventana de congestión actual por el retardo de propagación, o RTT mínimo, denominado *BaseRTT*. En la práctica, *BaseRTT* se estima como el RTT mínimo medido en la transmisión, normalmente a partir de los primeros mensajes enviados cuando la red aún no estaba cargada con esta conexión. La eficacia de Vegas depende en gran medida de una buena estimación de BaseRTT. Notoriamente, Vegas es capaz de detectar de esta manera la capacidad que soporta la red.

La *tasa real* es la tasa de envío actual, calculada dividiendo el tamaño de la ventana de congestión por el valor del RTT actual suavizado.

Diff es la diferencia entre la tasa esperada y la real. Debe estar entre los umbrales α y β, constantes que dependen de la implementación de Vegas, elegidos para mantener una tasa de envío adecuada que no infrautilice el ancho de banda disponible en la red pero que tampoco provoque congestión.

Para intentar mantener la tasa de envío entre estos dos umbrales, se modifica adecuadamente el tamaño de la ventana de congestión. Para cada RTT se comprueba *la diferencia diff*. Cuando este valor está por debajo del umbral α la ventana de congestión se incrementa en un paquete. Cuando excede el umbral β se disminuye en un paquete para disminuir la tasa (ya que esta condición se toma como una señal de congestión incipiente). Si el valor de la diferencia está en el rango aceptado el tamaño de la ventana permanece sin cambios.

Intuitivamente, cuanto más se aleja el rendimiento real del rendimiento esperado, más congestión que hay en la red, lo que implica que la tasa de envío debe reducirse. El *umbral* α desencadena esta disminución. Por otro lado, cuando la tasa de envío real se acerca demasiado a la esperada, la conexión corre el riesgo de no utilizar el ancho de banda disponible. El *umbral* β desencadena este aumento.

Gracias a esta estrategia Vegas es capaz de anticiparse a la congestión y a los eventos de pérdidas de paquetes a la vez que hace un uso muy responsable de los buffers de red, almacenando solo una cantidad mínima de paquetes en ellos sin dejar de aprovechar el ancho de banda disponible.

Control de congestión basada en análisis de tiempos para MPTCP: wVegas

wVegas [105] es el único algoritmo de control de congestión por análisis de tiempos (CCT) para MPTCP y está basado en TCP Vegas. En el trabajo preludio a esta tesis doctoral se hizo un exhaustivo análisis a la posibilidad de aplicación de CCT en , desarrollándose un algoritmo de gran similaridad a wVegas (cuando aún no se había dado a conocer), que fue presentado en el IETF. Se puede encontrar esta infromacion [107] y en [101].

Algoritmo 3.4: Reglas de aumento y disminución de CWND de wVegas

$$W \rightarrow \begin{cases} W_i + 1 & diff < \alpha K_i \\ W_I & \alpha K_i < diff < \beta K_i \\ W_i - 1 & diff > \beta K_i \end{cases} \quad \text{Comprobado cada RTT} \tag{15}$$

$$W_i \rightarrow W_i - \frac{W_i}{4} \quad \text{por dup-pérdida de ACK} \tag{16}$$

W_i se restablece en caso de que se agote el tiempo de espera

$$W_i = CWND \text{ de subflujo i} \tag{17}$$

$$RTT_i = \text{Ida y vuelta de subflujo i} \tag{18}$$

$$baseRTT_i = \text{Retraso de propagación de subflujo i} \tag{19}$$

$$diff_i = \text{Tasa esperada}_i - \text{Tasa real}_i \tag{20}$$

$$\text{Tasa real}_i = \frac{W_i}{RTT_i} \tag{21}$$

$$\text{Tasa esperada}_i = \frac{W_i}{baseRTT_i} \tag{22}$$

$$T_{POT\,i} = \frac{RTT_i \cdot baseRTT_i}{(RTT_i - baseRTT_i)} \tag{23}$$

$$K_i = \frac{T_{POT\,max} \cdot T_{POTi}}{\sum T_{POTj}} \sum \left(\frac{\sum T_{POTh}}{T^2_{POTj}} \right) \tag{24}$$

Cabe destacar que la integración de mecanismos de CCT en MPTCP no es trivial ya que el control de congestión de las distintas subconexiones tiene que estar interrelacionado (acoplamiento) para conseguir una utilización de los caminos responsable desde un punto de vista de reparto de recursos y de congestión de red global.

3.4. Diseño de un nuevo control de congestión para Multipath TCP

MPTCP requiere nuevos algoritmos de control congestión, diseñados específicamente para este nuevo protocolo, capaces de realizar un control de congestión eficiente. Actualmente existen pocos algoritmos CC para esta extensión de TCP (los ya mencionados LIA, BALIA, OLIA, Cubic y wVegas). Un objetivo de esta tesis doctoral ha sido la creación de un novedoso algoritmo de control de congestión para MPTCP que sea capaz de aportar los beneficios del avanzado control de congestión por análisis de retraso a la vez de permitir su competitividad y coexistencia con otros tipos de tráfico en las redes, solventando el gran problema de los ACCR.

Para la creación de este algoritmo se deben obligatoriamente que tener en cuenta las necesidades y requisitos específicos del control de congestión multicaminos para MPTCP. Como ya se ha mencionado, MPTCP requiere un equilibrio adecuado de la carga entre los subflujos, lo que representa una nueva responsabilidad para el algoritmo de control de la congestión no incluida en el control de la congestión TCP clásico. Además, esta distribución y equilibrio de carga debe respetar las tres reglas o pilares de diseño del control de congestión de MPTCP, definidas por los creadores de este nuevo protocolo y basadas en el Principio de Reparto Global de los recursos, un principio arquitectónico propuesto para el Internet del Futuro [98].

3.4.1. Objetivos y consideraciones de diseño

3.4.1.1 *Normas de diseño para el control de la congestión de MPTCP*

Debido a la filosofía de diseño de MPTCP, basada en el principio arquitectónico de reparto global de los recursos y en no competir deslealmente con conexiones de TCP

clásico, se han establecido varias reglas para la construcción de algoritmos de congestión. Por ello, el diseño de un algoritmo correcto de control de flujo para MPTCP debe perseguir los siguientes objetivos clave [113] o reglas de diseño establecidas por los creadores de la extensión MPTCP.

1) Mejorar el rendimiento sobre el uso de TCP clásico: *Conseguir como mínimo el mismo rendimiento que obtendría una conexión TCP utilizando la mejor ruta.*

Es decir, el rendimiento global de un flujo MPTCP (la suma de la velocidad de transmisión total o bien el ancho de banda utilizado por todos los subflujos) debe ser como mínimo lo mismo que conseguiría un único flujo TCP actuando en su lugar en el mejor de los caminos disponibles.

Incluso en el caso de que MPTCP obtenga exactamente el mismo rendimiento global que TCP en la mejor ruta, implica una mejora frente al uso de TCP: MPTCP consigue lo que TCP sólo en el mejor caso posible, cuando se enruta por el mejor camino, hecho que no implica el uso de TCP. TCP no puede elegir el mejor camino de un conjunto (potencialmente) disponible.

Una conexión MPTCP debería ocupar al menos el mismo ancho de banda que ocuparía en su lugar una única conexión TCP en la mejor ruta. Idealmente, la situación más justa para TCP significa ocupar exactamente la misma cantidad de ancho de banda. En cualquier caso, esta cuota no debería ser excesivamente mayor que la que obtendría TCP. MPTCP pretende ser justo con TCP y, por tanto, tomar una parte justa de la capacidad disponible en la red. Como excepción, en caminos vacíos, sin la presencia de otro tráfico y otras conexiones adicionales, es apropiado y conveniente ocupar todo el ancho de banda disponible.

Hay que tener en cuenta que esta mejora del rendimiento tiene una restricción de equidad.

MPTCP puede obtener potencialmente tanto rendimiento como la suma del rendimiento que cada subflujo puede alcanzar individualmente, ya que tiene la capacidad de agrupar la capacidad en todos los caminos. Sin embargo, este comportamiento no sería justo para los flujos TCP individuales, que sólo tienen la posibilidad de tomar parte de una ruta.

MPTCP pretende, por razones de equidad con los flujos TCP individuales, obtener un rendimiento similar al de una conexión TCP, aunque también pretende tener algún tipo de mejora. La situación óptima es obtener *exactamente* el mismo rendimiento que obtendría un flujo TCP utilizando la mejor ruta. Sin embargo, esto es difícil de conseguir en la práctica, pero representa una directriz. Además, hay que notar que en el caso especial del rendimiento en enlaces no compartidos con ningún otro tráfico un comportamiento lógico es tomar todo el ancho de banda del enlace, es decir no limitar el rendimiento global de ninguna manera ya que no perjudica al rendimiento de ningún flujo TCP.

2) No perjudicar a otras conexiones TCP aprovechando el hecho de que se podría acaparar abusivamente ancho de banda de varios caminos.

Los subflujos de una conexión MPTCP no deben perjudicar a otras conexiones TCP utilizando el mismo camino. Los subflujos MPTCP no deben tomar un ancho de banda mayor de un enlace que cualquier otra conexión TCP que se ejecute al mismo tiempo en el enlace. Y en caso de que varios subflujos de la misma conexión MPTCP estén actuando en el mismo enlace, no deben tomar en conjunto más cuota que la que obtiene un solo flujo TCP.

3) Reequilibrio del tráfico para mejorar la situación de congestión global en los caminos

Un flujo MPTCP debe desplazar el tráfico de sus rutas más congestionadas a las menos congestionadas, siempre que se cumplan los dos primeros objetivos.

Conseguir el cumplimiento de estas reglas implica una gran complejidad añadida en la construcción del algoritmo ya que como se ha visto no son triviales y tienen distintos casos especiales y excepciones que tener en cuenta.

3.4.2. Control de congestión acoplado

Otro punto importante a tener en cuenta en el diseño del algoritmo es que a raíz de todos los requisitos y objetivos para conseguir un control de congestión eficaz, cumplir con los tres pilares de diseño y conseguir un balanceo efectivo de la carga entre los caminos, el mecanismo de control de congestión tiene que estar interrelacionado entre las distintas subconexiones MPTCP, y por tanto depende de

todas ellas. Cada subflujo debe tener su propio estado de control de la congestión (es decir, cwnd), pero su rendimiento no puede ser independiente de los demás subflujos.

Para lograr la agrupación de recursos, es decir, que todo el conjunto actúe como uno solo, es necesario acoplar los bucles de aumento y disminución de todos los subflujos, obteniendo un control de congestión acoplado. Esto implica que las cantidades de aumento y disminución dependen del rendimiento del conjunto y son las mismas para todos los subflujos. Al efectuar un acoplamiento adecuado, los objetivos de diseño del control de la congestión deberían cumplirse, dando lugar a un rendimiento apropiado, a la equidad con respecto a otros flujos TCP y a un equilibrio de carga adecuado entre los subflujos.

3.4.3. Diseño de control de congestión híbrido

Como ya hemos visto, normalmente el control de la congestión TCP y MPTCP se basa en la pérdida: es necesario perder paquetes de datos periódicamente para regular la velocidad de transmisión. En consecuencia, la congestión y la pérdida son por tanto inherentes e inevitables [110].

En contraste, el control de la congestión basado en el análisis de tiempos de transmisión presenta enormes ventajas en comparación. Permite una detección de la congestión más precisa que permite una acción preventiva más rápida contra la congestión antes de que se produzcan pérdidas de paquetes (evento muy costoso en términos de rendimiento), y una regulación muy afinada y precisa del flujo [105][109]. No sólo ahorra el coste de la pérdida de rendimiento en la medida de lo posible, también presenta una acción preventiva más eficaz contra la congestión e induce un menor retardo [9]. En especial, en MPTCP una regulación más fina de la tasa de transmisión puede permitir un mejor, más preciso y más justo equilibrio de carga entre los subflujos. Sin embargo, el control de congestión clásico basado en el retardo [11], presenta el inconveniente de un rendimiento muy pobre al compartir enlaces con tráfico con CC basado en pérdidas. El control de congestión basado en pérdidas es más agresivo a la hora de acaparar el ancho de banda disponible en los enlaces de red. Por ello el tráfico con CCR tiene una CWND y uso del ancho de banda mínimo

cuando coexiste con tráfico CCP, el cual acapara prácticamente la totalidad del ancho de banda disponible.

La solución para obtener los beneficios del CCR sin su gran problema de rendimiento al compartir enlaces con tráfico con CCP (mayoritario en las redes) puede encontrarse en la creación de un control de congestión híbrido que combine aspectos de ambos tipos de control de congestión (basado en pérdidas y basado en análisis de tiempos). Existen algunos intentos de creación de algoritmos híbridos en TCP, como Microsoft Compound [114], con parte de su CWND basado en Vegas y parte en Reno, o un esquema de AIMD considerando elementos de detección precoz de pérdidas. Sin embargo no es así en MPTCP donde solo wVegas [105] utiliza detección por tiempos pura.

En el trabajo presentado en esta tesis doctoral se ha intentado mejorar el control de congestión de MPTCP, una función crítica para el rendimiento de transmisión y evitar el colapso de red, aportando los grandes beneficios del CCR , creando un nuevo tipo de CC, el control de congestión híbrido, y un nuevo algoritmo capaz de.

Esto podría permitir los beneficios de una detección temprana de la congestión incipiente, antes de que se produzca la pérdida, y un rendimiento adecuado que interopera con las implementaciones basadas en pérdidas.

Hemos diseñado DAIMD, un novedoso control de congestión híbrido para Multipath TCP. DAIMD permite una acción preventiva contra la congestión más eficaz que las implementaciones de MPTCP basadas en pérdidas, y un rendimiento adecuado con tráfico de fondo basado en pérdidas. DAIMD se basa en el AIMD basado en el retardo pero presenta un criterio diferente para activar la disminución de la tasa de transmisión. Se ha implementado este nuevo algoritmo en el kernel de Linux y evaluamos su rendimiento en simulaciones utilizando una pila de red real en lugar de modelos [115]. Esto permite resultados muy precisos, considerados equivalentes a los conseguidos en redes reales. Investigamos si DAIMD presenta los beneficios esperados del control de congestión híbrido, y se comporta como una implementación funcional de MPTCP, cumpliendo los objetivos de control de congestión de MPTCP.

3.4.4. Algoritmo DAIMD: control de congestión híbrido

En el trabajo de esta tesis se ha implementado un esquema híbrido de control de congestión que utiliza la estrategia AIMD de los algoritmos basados en pérdidas para no perder competitividad frente a tráfico agresivo concurrente en la red, y a su vez un criterio de reducción de flujo por análisis de tiempos. Este diseño persigue dos características altamente ventajosas que no se encontraban juntas en los algoritmos MPTCP existentes. Por un lado, la primera característica sería permitir un control de congestión inteligente y eficiente basado en análisis de tiempos, que permitiría un mejor reparto de recursos y evitar la aparición de pérdidas inherentes, muy costosas en cuestión de rendimiento. Y por otro lado, un funcionamiento apropiado para no ceder la práctica totalidad del ancho de banda a tráfico más agresivo en los canales o rutas que usa la conexión. Se siguen las 3 reglas de diseño de un algoritmo Multipath TCP de congestión y se añade funcionalidad específica para el análisis de tiempos y control competitivo del flujo de transmisión. Está parcialmente basado en la adaptación del algoritmo híbrido para TCP clásico AIMD con retardo.

El algoritmo resultante, DAIMD, sigue un criterio basado en tiempos para la disminución multiplicativa de la ventana de congestión y el flujo de datos, mientras que presenta el aumento aditivo, el acoplamiento y el comportamiento general de LIA [116], el primer algoritmo propuesto por el IETF para TCP Multipath.

Desarrollamos nuestro propio criterio para desencadenar la disminución multiplicativa, tras inspirarnos en los aspectos del criterio de varios algoritmos basados en el retardo. En el caso de detección precoz de una pérdida inminente se aplica el factor de reducción como coeficiente reductor. En caso de pérdida (no inherente, pero que podría darse en caso de alta congestión) también se activa una disminución multiplicativa, pero siguiendo en este caso la regla de LIA para la pérdida y no el factor de reducción.

El factor de reducción se ha escogido para que el rendimiento de DAIMD sea similar al de LIA, a pesar de que DAIMD detecta antes la congestión. DAIMD detecta la necesidad de una disminución multiplicativa antes de que se produzca la pérdida, por lo que obtiene un valor superior de la ventana de congestión menor que LIA en las mismas condiciones. DAIMD debería tener una reducción menos agresiva, ya que la

acción preventiva contra la congestión impide también alcanzar un tamaño de ventana de congestión mayor.

Algoritmo 3.5: Reglas de aumento y disminución de CWND de MPTCP DAIMD

Reglas para cada subflujo r:
Incrementar en cada ACK de subflujo r

$$cwnd_r \leftarrow cwnd_r + \min(1/cwnd_r, \alpha/cwnd_{total}) \quad (25)$$

Disminuir

$cwnd_r \leftarrow cwnd_r \cdot 0.7$ al detectar retraso de congestión (26)

$cwnd_r \leftarrow cwnd_r \cdot 0.5$ en cada pérdida de subflujo r (27)

$$\alpha = \max\left(\frac{cwnd_j}{rtt_j^2}\right) / \left(\sum \frac{cwnd_i}{rtt_i}\right)^2 \quad (28)$$

$$cwnd_{total} = \sum cwnd_i \quad (29)$$

$rtt_r, cwnd_r$: tiempo de ida y vuelta y CWND en camino r (30)

3.5. Evaluación del algoritmo DAIMD

Para evaluar el correcto funcionamiento de este nuevo control de congestión para MPTCP se han realizado múltiples experimentos y simulaciones. En este documento se presentan varios experimentos y mediciones asociadas considerados altamente representativos para el análisis de su funcionamiento y comportamiento ante situaciones de congestión, donde se puede observar la acción preventiva ante pérdidas, regulación del flujo de datos de transmisión y su rendimiento coexistiendo con tráfico agresivo en la red.

3.5.1. Implementación del algoritmo

El algoritmo DAIMD ha sido implementado en un sistema operativo real [115]. He implementado el nuevo control de congestión híbrido como un nuevo módulo de la pila de red del kernel de Linux. En aras de la simplicidad, no se han implementado otras operaciones MPTCP (señalización) ni la extensión del protocolo TCP, sino únicamente el control de congestión ya que resulta suficiente para evaluar el

algoritmo y el control de flujo resultante - la señalización y la fase inicial handshake no influyen en el comportamiento del control del flujo de datos.

Este algoritmo se ha programado en C solventando las limitaciones de la programación de módulos en el kernel de linux, donde muchas funciones básicas numéricas o tipos de datos aún no están cargados, y solo es posible utilizar operaciones básicas y el tipo de datos entero para implementar complejos sumatorios en los que se basa el algoritmo.

3.5.2. Preparación y realización de los experimentos

Los experimentos se han realizado con el simulador de redes más extendido en la comunidad científica (NS3) y utilizando código real de la pila de red del sistema operativo de los host finales en lugar de modelos, lo que proporciona resultados considerados equivalentes a los obtenidos en redes reales.

El algoritmo se ha implementado en un sistema operativo real (kernel de Linux) como un módulo de la pila de red, y el código real de esta parte del kernel se ha empleado en NS3 para la simulación de tramisiones de datos en distintos escenarios, en lugar de utilizar un modelo, como típicamente se emplea en muchos análisis de protocolos. A diferencia del uso de modelos para la simulación, el uso de código de pila de red real proporciona resultados extremadamente precisos, que se consideran equivalentes a los obtenidos en redes reales [92].

Se han diseñado e implementado en NS3 varios escenarios de tráfico para realizar una evaluación básica del algoritmo. En este documento se muestran los resultados obtenidos en escenarios con dos caminos ideales de red y una conexión MPTCP que emplea estos dos caminos con sus dos subconexiones (una subconexión MPTCP en cada camino), como puede verse en la Figura 3.4. Estos dos caminos en la red conectan pues a los dos equipos que mantienen una conexión MPTCP de dos subflujos. Cada camino es un enlace ideal de red sin factor de pérdida y su cola o buffer tiene la misma capacidad que el valor del producto de su ancho de banda por el retraso de transmisión que induce. La elección de este tamaño de buffer se debe a que es el considerado óptimo y típico en un enlace de red para circunstancias de tráfico normales, ya que permite el uso de TCP Reno de manera óptima. Cada host mantiene una sola conexión MPTCP; todas las subconexiones MPTCP que se simulan

y analizan pertenecen a esta misma conexión. Las fuentes son generadores de tráfico que comienzan a enviar paquetes en un mismo instante exacto de tiempo de inicio.

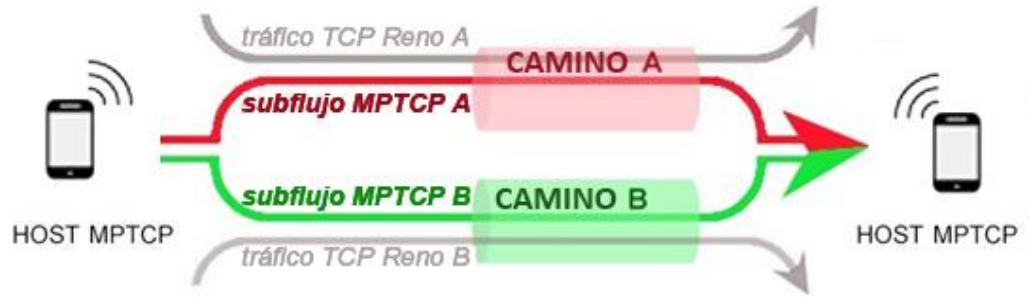


Figura 3.4 Escenario de tráfico genérico para la simulación, que se particulariza en escenarios con distintas características de tráfico, capacidad de los enlaces y retraso base de transmisión

Esta conexión MPTCP hace uso de distintos algoritmos de control de congestión según el experimento realizado, y puede contar con la presencia o no de tráfico externo de tipo CCP compartiendo los recursos de cada enlace de red con la conexión MPTCP, según el escenario concreto. Las características de retraso de transmisión y capacidad de cada subcamino, así como la presencia o no de tráfico adicional basado en pérdidas (Reno) son distintas en cada simulación individual, adoptando los valores especificados en la Tabla 3.1 donde se observan las particularizaciones concretas de cada escenario.

Las especificaciones del escenario de tráfico de dos caminos se indican en la tabla siguiente, las cuales varían en cada tanda de simulaciones.

Tabla 3.1 Particularizaciones del escenario de tráfico

ESCENARIO A **2 Canales con diferente capacidad y mismo retraso base de transmisión**				**ESCENARIO A1**	**ESCENARIO A2**
	Capacidad	Retraso base de transmisión	Tamaño del buffer	Tráfico externo	
RUTA DE RED A	**10 Mbps**	50 ms	500 Kb	**NO**	**Conexión TCP Reno**
RUTA DE RED B	**5 Mbps**	50 ms	250 Kb	**NO**	**Conexión TCP Reno**
ESCENARIO B **2 Canales con diferente retraso base y misma capacidad**				**ESCENARIO B1**	**ESCENARIO B2**
	Capacidad	Retraso base de transmisión	Tamaño del buffer	Tráfico externo	
RUTA DE RED A	5 Mbps	25 ms	125 Kb	**NO**	**Conexión TCP Reno**
RUTA DE RED B	5 Mbps	50 ms	250 Kb	**NO**	**Conexión TCP Reno**
ESCENARIO C **2 Canales con igual retraso base y misma capacidad**					**ESCENARIO CT**
	Capacidad	Retraso base de transmisión	Tamaño del buffer		Tráfico externo
RUTA DE RED A	5 Mbps	25 ms	125 Kb	-	**Conexión TCP Reno**
RUTA DE RED B	5 Mbps	50 ms	250 Kb	-	**Conexión TCP Reno**

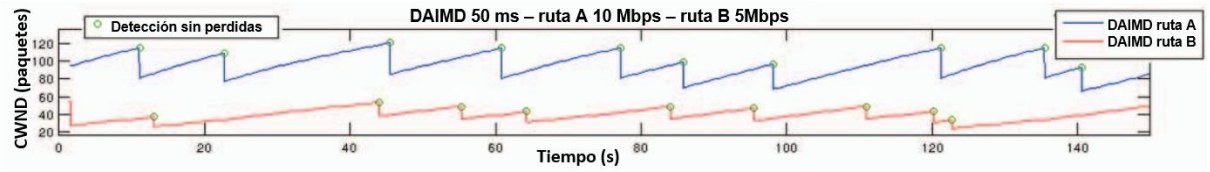
3.5.3. Resultados

3.5.3.1 *Resultados en escenarios sin tráfico externo*

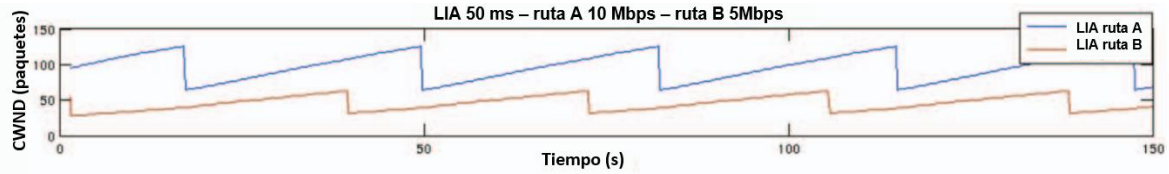
Los enlaces de red o caminos en este caso solo están utilizados por una subconexión o subflujo de la conexión MPTCP analizada.

Resultados en 2 caminos con distinta capacidad e igual retraso de transmisión

ESCENARIO A
2 caminos con diferente capacidad y mismo retraso de transmisión
Camino A – 10Mbps – 50ms
Camino B – 5Mbps – 50ms



(a)

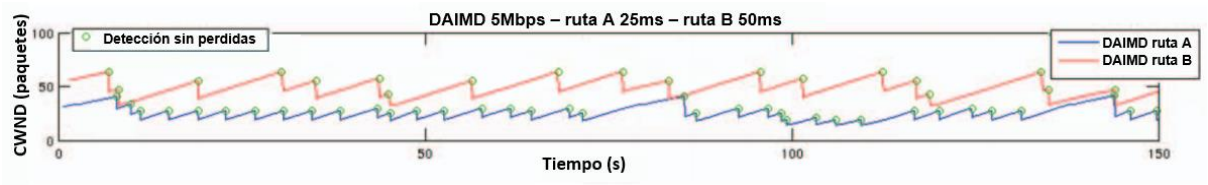


(b)

Figura 3.5 Comparación del comportamiento de DAIMD y LIA en escenarios idénticos sin tráfico externo con dos caminos de diferente capacidad (10 Mbps y 5 Mbps).

Resultados en·2 caminos con igual capacidad y distinto retraso de transmisión

ESCENARIO B
2 caminos con diferente retraso de transmisión y misma capacidad
Camino A – 10Mbps – 50ms
Camino B – 5Mbps – 50ms



(a)

(b)

Figura 3.6 DAIMD y LIA en escenarios idénticos sin tráfico externo con 2 rutas con diferente retraso de transmisión.

Tabla 0.2 Ancho de Banda utilizado por cada subconexión (en Mbps)

Conexión MPTCP DAIMD	**2 Canales con diferente capacidad y mismo retraso de transmisión** Ruta A - 10Mbps - 50ms Ruta B - 5Mbps - 50ms	**2 Canales con diferente retraso base y misma capacidad** Ruta A - 5Mbps - 25ms Ruta B - 5Mbps - 50ms
Subconexión A	9.4	4.5
Subconexión B	4.2	4.6
Ancho de banda total de MPTCP	13.6	9.1

En las Figuras 3.5 y 3.6 se puede apreciar el comportamiento del algoritmo en enlaces vacíos, sin la influencia de otro tráfico compartiendo el enlace y sus recursos. Estos canales tienen diferentes características de retraso base de transmisión y capacidad que están claramente especificadas en las tablas y figuras que muestran los resultados asociados. Para comparar el control de la congestión de DAIMD con su algoritmo equivalente basado en pérdidas, también se muestra el rendimiento de LIA en escenarios idénticos. Como se puede ver en la definición del algoritmo en una sección anterior, DAIMD utiliza los mismos mecanismos que LIA excepto en la detección de pérdidas. Se puede observar que el rendimiento de DAIMD es muy similar al de LIA, pero con una menor oscilación pico a pico, más irregular y con mayor frecuencia. El tamaño máximo de la ventana de congestión en las mismas condiciones de ruta es ligeramente inferior para DAIMD que para LIA, ya que DAIMD detiene el aumento del CWND antes que LIA, debido a una detección más temprana de la congestión. Cada detección precoz de la congestión, antes de que una pérdida de paquetes inminente se produzca, está indicada en las imágenes con un círculo. Por otro lado, los picos sin círculo representan eventos en los que sí ha habido pérdida de paquetes.

No se produce ninguna pérdida en las transmisiones DAIMD después de la fase de inicio lento, lo que demuestra una gran eficacia del control de la congestión a la hora de prevenir pérdidas. Por otro lado, un control de la congestión basado en tiempos óptimo debe actuar contra la congestión reduciendo la tasa con la suficiente antelación para evitar pérdidas sin dejar tampoco mucho margen temporal de anticipación al ejecutar la reducción de la tasa de transmisión en respuesta. Una activación inadecuada e imprecisa puede conducir a la infrautilización del ancho de banda y a la incapacidad de competir con otras conexiones en la red por una parte justa del ancho de banda disponible. En este sentido, DAIMD es capaz de mantener un rendimiento adecuado en cada uno de los trayectos o caminos (véase la Tabla 3.2), lo que sugiere una respuesta temporal apropiada en su mecanismo de detección de pérdidas y ajuste de flujo. Por lo tanto, DAIMD cumple el objetivo de diseño del control de congestión de MPTCP para caminos no compartidos (utilización apropiada de la capacidad del canal) y se comporta como un control de congestión funcional para MPTCP con una acción eficaz y preventiva contra las pérdidas.

3.5.3.2 *Resultados en rutas compartidas con tráfico externo*

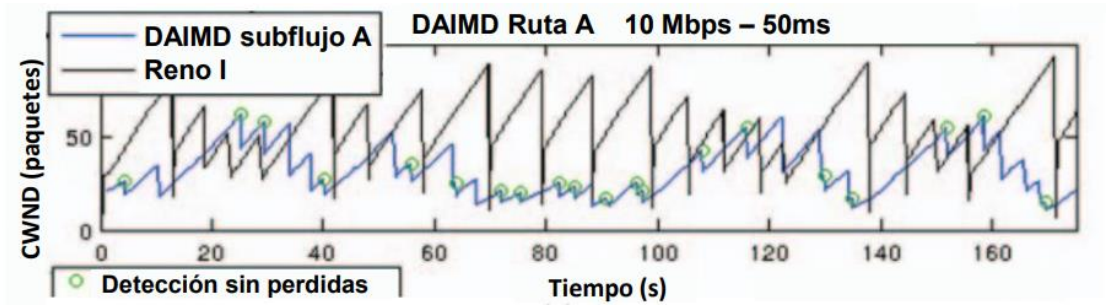
Las Figuras 3.6, 3.7 y 3.8 muestran el rendimiento de DAIMD y LIA en escenarios con tráfico adicional. Elegimos Reno, la implementación estándar de TCP, como tipo de tráfico añadido. Una única conexión TCP Reno se ejecuta en cada uno de los caminos –lo que permite analizar con mayor claridad la influencia del tráfico sobre los subflujos MPTCP DAIMD que utilizando en su lugar un conjunto de conexiones externas.

ESCENARIO A2
2 caminos con diferente capacidad y mismo retraso de transmisión
Tráfico de 1 conexión TCP Reno en cada camino
Camino A – 10Mbps – 50ms
Camino B – 5Mbps – 50ms

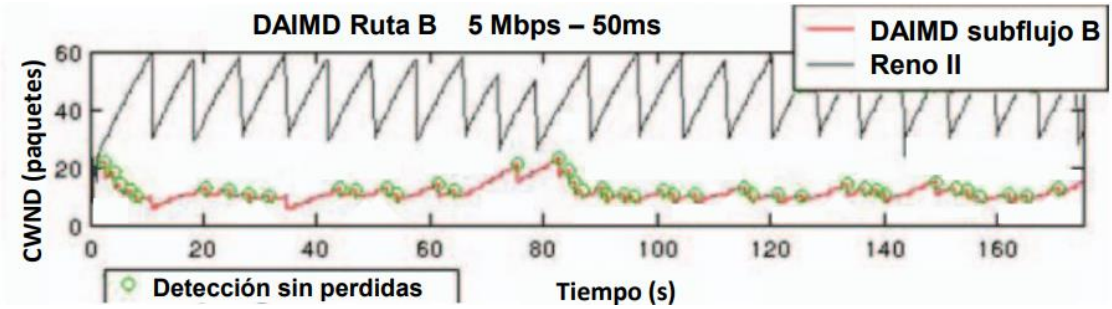
ESCENARIO B2
2 caminos con diferente retraso de transmisión y misma capacidad
Tráfico de 1 conexión TCP Reno en cada camino
Camino A – 5Mbps – 50ms
Camino B – 5Mbps – 25ms

ESCENARIO C2
2 caminos idénticos con el mismo retraso de transmisión y capacidad
Tráfico de 1 conexión TCP Reno en cada camino
Camino A – 5Mbps – 50ms
Camino B – 5Mbps – 50ms

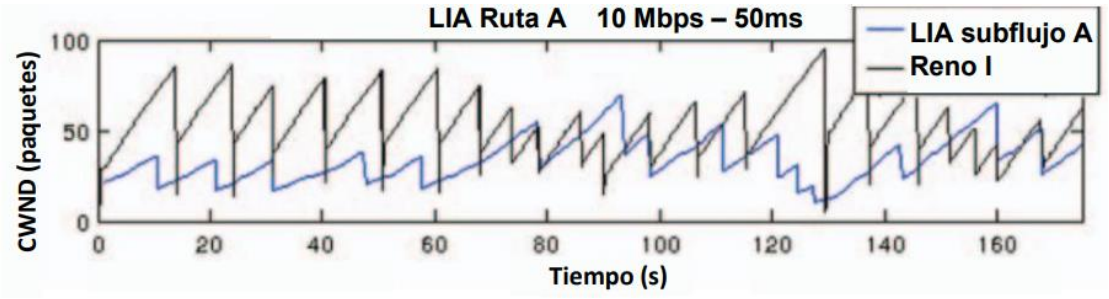
Resultados en escenario con caminos de distinta capacidad



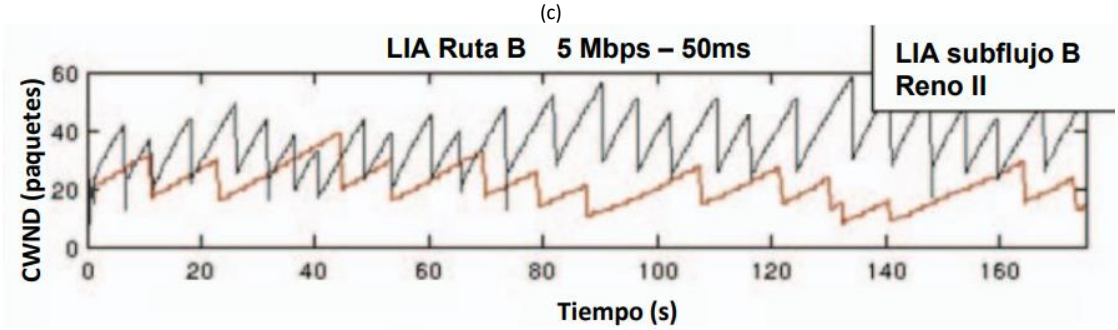
(a)



(b)



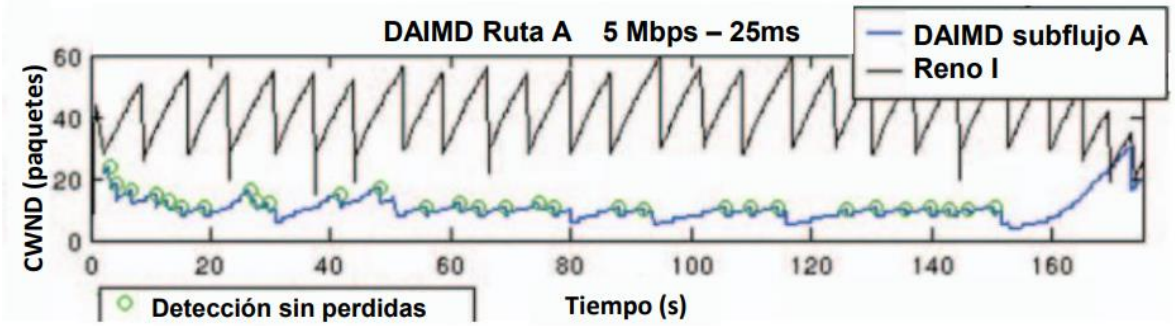
(c)



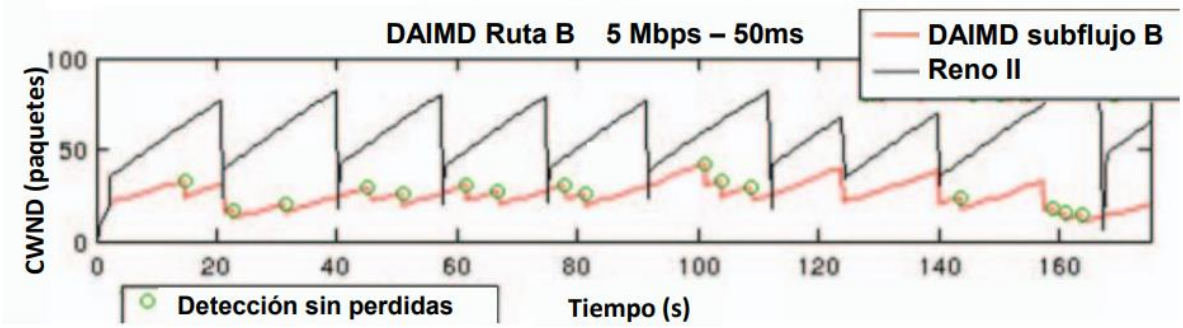
(d)

Figura 3.7 Conexiones DAIMD y LIA en dos canales con distinta capacidad y tráfico externo

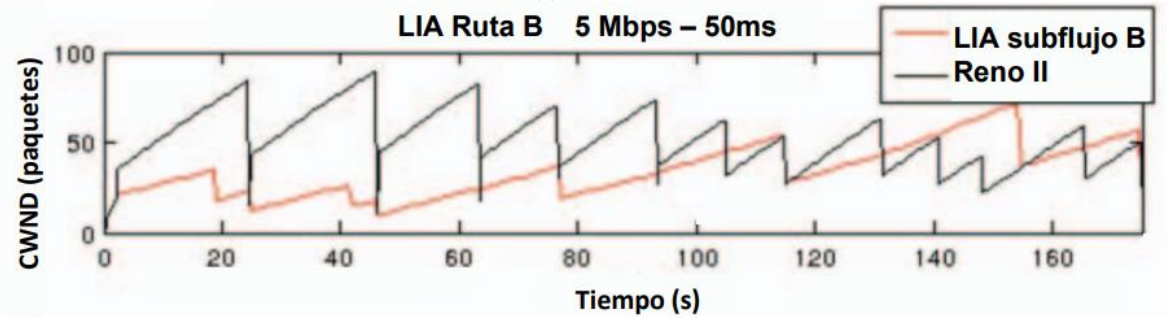
Resultados en escenario con caminos con distinto retraso base



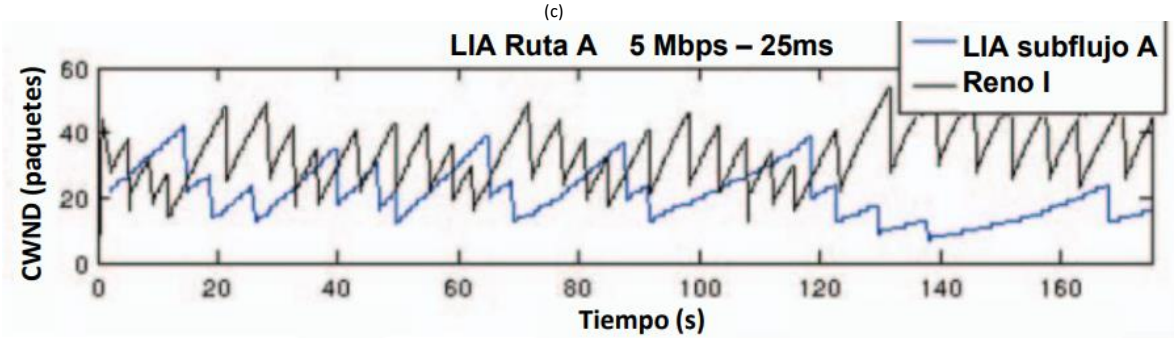
(a)



(b)



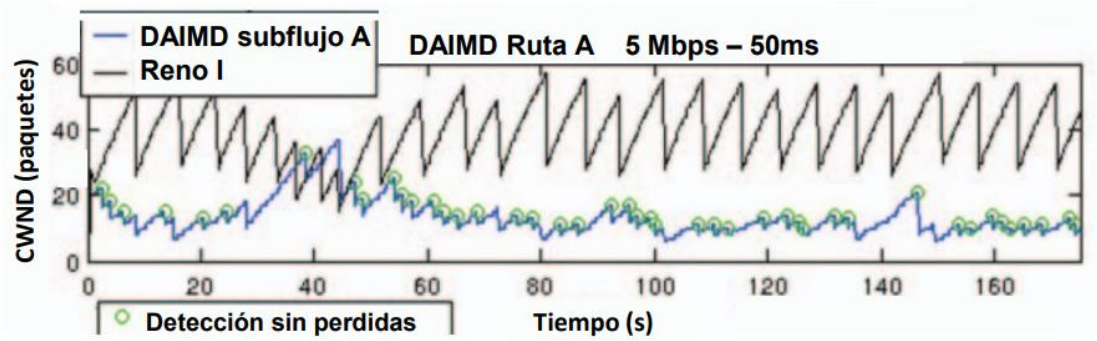
(c)



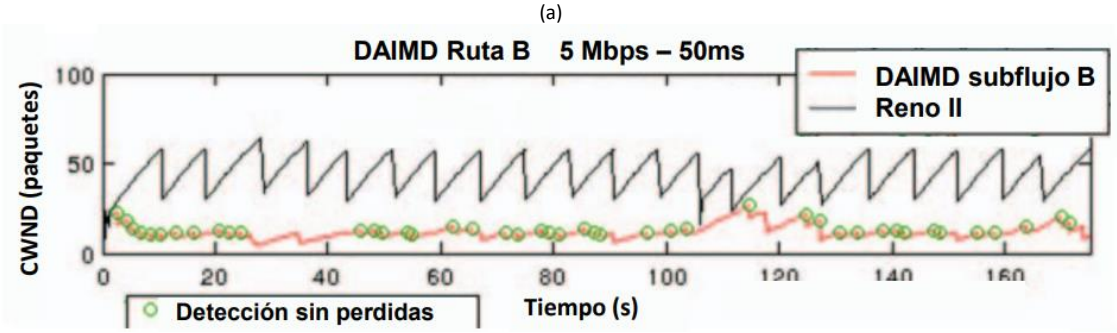
(d)

Figura 3.8 Conexiones DAIMD y LIA en dos canales con distinto retardo de transmisión base y tráfico externo

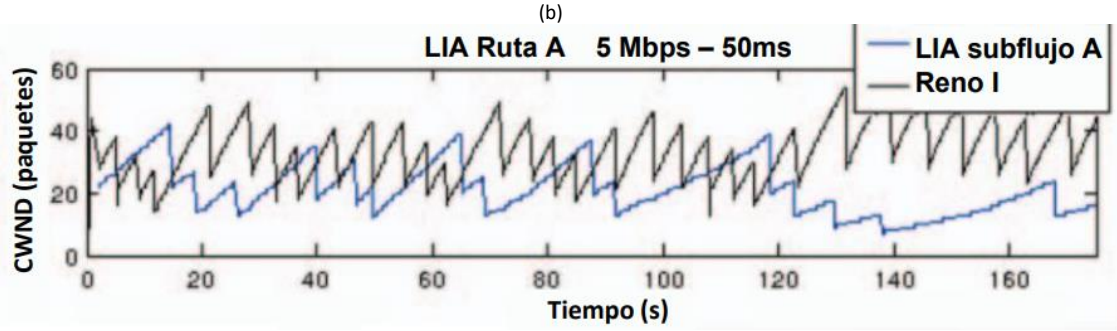
Resultado en escenario de caminos iguales



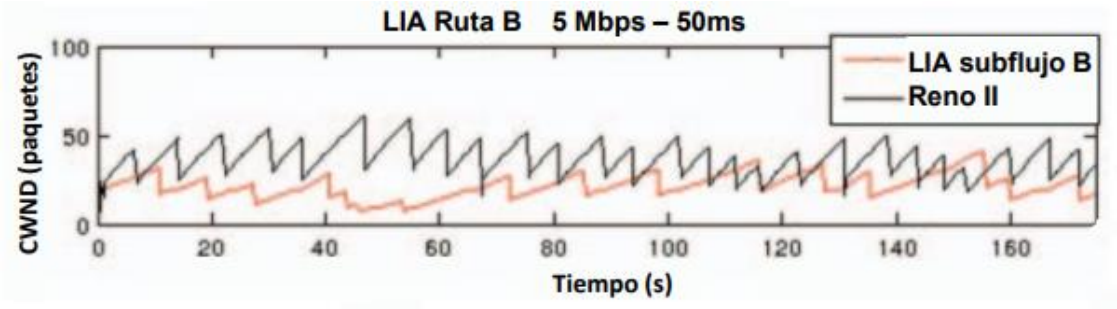
(a)



(b)



(c)



(d)

Figura 0.9 Conexiones DAIMD y LIA en dos canales idénticos con tráfico externo

Tabla 3.3 Tasa de envío y utilización del canal por cada conexión y subconexión (en Mbps)

	Caminos con diferente capacidad			Caminos con diferente retraso			Caminos iguales		
	DAIMD	LIA	Reno (DAIMD)	DAIMD	LIA	Reno (DAMID)	DAIMD	LIA	Reno (DAIMD)
Ruta A	3.4	3.6	5.8	1.4	1.8	2.9	1.3	1.5	3.5
Ruta B	1	1.7	3.7	1.1	1.6	2.8	1.2	1.7	3.7
Total MPTCP	4.4	5.3	mptcp cuota ideal: 5	2.5	3.4	mptcp cuota mínima ideal: 2.5	2.5	3.2	mptcp cuota mínima ideal: 2.5

3.5.4. Evaluación global de los resultados

Los resultados muestran que DAIMD se comporta de forma similar a LIA. Consideramos que los objetivos de control de la congestión del diseño de TCP multirruta se consiguen en las simulaciones, pero no estrictamente en cuanto al primer objetivo. Como se puede ver en los gráficos y en la Tabla 3.3, DAIMD toma casi el mismo ancho de banda que obtendría un único flujo TCP en el mejor camino. El reparto justo ideal, según el principio de agrupación de recursos y los objetivos de equidad del diseño de TCP multirruta, es exactamente el que obtendría una conexión TCP individual. En el escenario con rutas con diferentes capacidades, DAIMD obtiene un rendimiento inferior al ancho de banda equitativo esperado (5Mbps). Sin embargo, DAIMD obtiene una utilización alta y aceptable del ancho de banda que le corresponde idealmente ideal. Aun no cumpliendo de manera estricta el primer objetivo de diseño, el resultado es lo suficientemente bueno como para considerarse que el objetivo de rendimiento de MPTCP se ha alcanzado aceptablemente. En las demás simulaciones, el rendimiento de DAIMD alcanza exactamente esta cuota ideal, a diferencia de LIA, en las mismas condiciones de trayectoria. LIA por su parte cumple el primer objetivo, pero supera su cuota ideal de recursos.

El segundo objetivo de diseño también se cumple (no obtener más capacidad que un único flujo TCP en una ruta compartida), como puede verse en la Tabla 3.3. En los gráficos 3.7a, 3.7c, 3.7d, 3.8c, 3.8d y 3.9a se puede observar que tanto DAIMD como LIA obtienen más rendimiento que la conexión Reno que comparte el mismo subcamino durante un instante en pocas y excepcionales ocasiones, lo que afecta

poco al rendimiento medio de los flujos. Los resultados del rendimiento medio demuestran que este objetivo de MPTCP se consigue, a pesar de estas situaciones momentáneas. El tercer objetivo de diseño es el equilibrio de carga adecuado entre los subflujos. Al igual que LIA, DAIMD utiliza más los mejores caminos, con más ancho de banda disponible y menos congestión, y menos los peores o más congestionados. Pero diferentemente, en estas simulaciones DAIMD quita comparativamente más tráfico de los caminos más congestionados que LIA. La utilización del peor camino, con respecto al uso global de los caminos, es proporcionalmente menor en DAIMD que en LIA. Este hecho sugiere que debido a su mayor sensibilidad al nivel de ocupación del enlance y a la congestión gracias al análisis de tiempos, y su forma menos brusca y precisa de reajustar CWND, es capaz de reaccionar mejor para reequilibrar el tráfico y minimizar la congestión entre caminos, en términos de tiempo y de ajuste de la tasa de transmisión.

La gran sensibilidad al nivel de congestión que tiene DAIMD (gracias a los mecanismos de análisis de tiempos) parece permitirle desplazar más tráfico que LIA de los enlaces congestionados. Respecto al tercer objetivo de diseño, el balanceo de congestión entre caminos, DAIMD lo logra con mayor eficacia que LIA, y se acercaría más a los objetivos del principio de agrupación de recursos.

En los dos casos, pero muy especialmente con DAIMD, MPTCP contribuye a una distribución más justa y eficiente de los recursos entre los flujos de la red (incluyendo también las conexiones no MPTCP, es decir en este caso de TCP Reno), como efecto del alivio de la congestión en los enlaces más congestionados al desplazar el tráfico y una distribución adecuada de la carga de datos entre sus subconexiones. Esto no sólo resulta ser beneficioso para el rendimiento de la propia conexión MPTCP, sino también indirectamente para las conexiones que comparten enlaces con subconexiones MPTCP. Se puede observar, en este sentido, que como efecto secundario a esta acción los flujos que comparten enlaces con MPTCP tienden a igualar, hasta cierto punto, el ancho de banda que utilizan o cuota de recursos, ayudando a una distribución más equitativa de los recursos globales de red. El uso de nuestro control de congestión híbrido en MPTCP puede reforzar este efecto, ya que mejora el equilibrio de carga.

Otro aspecto importante observado es que DAIMD presenta algunos episodios de pérdidas en estas simulaciones al compartir el enlace con tráfico agresivo (con CCP), aunque la gran mayoría de eventos potenciales de pérdidas son evitados. Esto era un

efecto esperable al compartir enlaces; el uso menos responsable de las colas de conexiones de CCP obliga a una sobrecarga periódica de las colas, a la pérdida de paquetes y a la congestión de la red. En ese tipo de situación de congestión, la pérdida es más difícil de evitar para el control de la congestión basado en el retardo. DAIMD es capaz de evitar las pérdidas en la mayoría de las ocasiones anticipando la sobrecarga de la cola y activando la disminución multiplicativa. Esto ahorra el coste de las pérdidas y las retransmisiones adicionales al rendimiento de la conexión. En comparación con el control de la congestión basado en las pérdidas, DAIMD presenta un uso más responsable de las colas de almacenamiento o buffers, previniendo la sobrecarga y las pérdidas y, en consecuencia, induciendo menos retraso debido a las retransmisiones causadas por las pérdidas o retraso por alta utilización de las colas.

3.6. Conclusiones

El algoritmo diseñado, DAIMD, ha demostrado en los experimentos ser un algoritmo efectivo para MPTCP, con un novedoso enfoque híbrido de control de la congestión, basado en AIMD con retardo y con un mecanismo diferente para detectar la congestión incipiente mediante el análisis del retardo. Esto le convierte en el primer algoritmo de control de congestión para MPTCP con un control de congestión híbrido y el segundo basado en análisis de tiempos, ya que implementa mecanismos de control de flujo basados en este sistema.

Siguiendo un esquema AIMD, el esquema de aumento se basa en LIA, el primer algoritmo de congestión basado en pérdidas para TCP multirruta propuesto por el IETF, así como el acoplamiento, el equilibrio de carga y la funcionalidad general. La disminución multiplicativa sigue el esquema general de AIMD basado en el retardo, pero con un criterio diferente para activar la disminución. El factor de reducción se ajusta para compensar el efecto de la detección temprana de la congestión, en comparación con la acción tardía de ajuste tras una detección de pérdidas.

En los casos estándar probados con simulaciones, DAIMD demuestra comportarse adecuadamente en términos de evitación de pérdidas, detección de congestión incipiente, equidad, adecuación, rendimiento en enlaces inactivos, así como la interoperabilidad con flujos basados en pérdidas en enlaces compartidos, los objetivos de control de la congestión de TCP multirruta, incluyendo la agrupación y reparto de recursos, y el uso responsable de las colas.

DAIMD demuestra ser capaz de lograr los beneficios esperados de un esquema basado en el retardo, como la evitación de pérdidas, la equidad intraprotocolo, la acción proactiva contra la congestión y la baja inducción de retardo.

Además, DAIMD posee la capacidad de interoperar en condiciones justas con flujos basados en pérdidas, lo que es imposible para el control de congestión clásico basado en el retardo. Sólo el control de congestión híbrido, como Compound y el AIMD basado en el retardo, son capaces de lograr esta característica deseable al tiempo que aplican una acción preventiva y de respuesta contra la congestión mediante el uso de la detección basada en el retardo de la congestión. DAIMD es la primera propuesta de control de congestión híbrido para TCP multirruta. Su acción proactiva contra la congestión evita hasta cierto punto la sobrecarga de las colas y, por tanto, presenta un uso más receptivo de las mismas, induciendo menos retardo, y ahorra el importante coste en rendimiento de las pérdidas en la medida en que es posible.

Las simulaciones han demostrado una importante reducción de las pérdidas, e incluso han evitado el total de las mismas en la ausencia de tráfico basado en Reno.

DAIMD se comporta satisfactoriamente como un algoritmo de congestión MPTCP funcional, ya que cumple los objetivos de rendimiento y equidad de MPTCP. El primer objetivo de diseño exige que toda una conexión MPTCP ocupe al menos el mismo ancho de banda que ocuparía una conexión TCP en la mejor ruta o enlace disponible para la conexión MPTCP, objetivo que DAIMD consigue en términos generales. En algunas simulaciones, DAIMD se acerca más que LIA al reparto justo ideal, es decir, a exactamente la misma capacidad que obtendría un flujo TCP en el mejor camino. El segundo objetivo se refiere a la equidad para TCP en cada ruta individual: un subflujo MPTCP no debe tomar más ancho de banda disponible que cualquier flujo TCP que comparta la misma ruta, y DAIMD lo cumple en todas las simulaciones. Por otro lado, como caso especial de esta regla, en los enlaces no compartidos es conveniente que se cumpla toda la capacidad disponible, algo que DAIMD ha realizado. El tercer objetivo de diseño que establece que la carga debe estar adecuadamente equilibrada entre los caminos disponibles también ha sido satisfecho en términos generales: los resultados sugieren que, comparativamente, DAIMD equilibra el tráfico incluso mejor que LIA, ya que en los escenarios genéricos analizados desplaza más tráfico de la ruta más congestionada y utiliza proporcionalmente más la mejor ruta. Esto puede verse en la Tabla 3.3.

Los resultados sugieren que DAIMD puede mejorar la equidad de LIA con respecto a TCP en algunos aspectos, ya que en algunos casos el rendimiento de DAIMD está más cerca del reparto equitativo ideal que la tasa de LIA y DAIMD hace una distribución de la carga más justa que LIA en los casos estudiados.

Respecto a su importancia en el ámbito de IoT, y de la interoperabilidad técnica, se ha de destacar que el protocolo MPTCP está ampliamente usado en los teléfonos inteligentes en la actualidad, puede ser utilizado por pasarelas IoT de red (pasarelas inteligentes), así como por dispositivos IoT que soporten el uso de TCP. Y que por otro lado se considera que será probablemente un protocolo clave en entornos 5G y 6G debido a su capacidad de mejora de la eficiencia de energía y rapidez de transmisión de datos [85].

Como ventajas adicionales, hay que destacar que este tipo de control de congestión al ser aplicado en TCP multirruta tiene una acción global contra la congestión al mover el tráfico de los peores caminos, los más congestionados, a los mejores caminos, los menos congestionados, lo que alivia la congestión en la red [6]. De este modo, no sólo la conexión MPTCP consigue una mayor eficiencia, una mejor distribución de los recursos y evitar la congestión. Además, los otros flujos que comparten enlaces con los subflujos MPTCP se benefician de esta acción, ya que la congestión general se reduce al redirigir el tráfico fuera de los enlaces más congestionados. Otras ventajas debidas a la utilización de múltiples caminos, la cual permite eludir las limitaciones debidas a la dependencia de un solo camino en TCP clásico son [92]:

- Mejora del rendimiento (ancho de banda de la conexión) frente a TCP
- Más robustez - Al utilizar varias rutas, la conexión es más resistente a los problemas en una ruta concreta. Incluso en caso de fallo de la ruta, la conexión se mantiene tal cual utilizando también otras rutas de trabajo.
- La fiabilidad es mayor que la de los propios componentes de la red de manera individual debido a la existencia de otros caminos con otros recursos.
- Flexibilidad para la acomodar picos de tráfico.

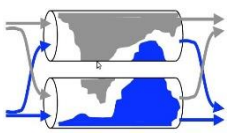


Figura 3.10 Flexibilidad multitrayectoria para acomodar picos de tráfico.

El uso de algoritmos MPTCP conduce indirectamente a una mejor distribución de los recursos de la red entre el MPTCP y los flujos que comparten enlaces con el MPTCP, y a una menor congestión general en la red ya que a diferencia del TCP clásico, que no puede mejorar una situación de congestión y sólo puede adaptarse a ella reduciendo su tasa de transmisión, MPTCP puede aliviar los enlaces congestionados y el equilibrar el uso de recursos en la red. Esto representa una nueva forma de control de la congestión que podría tener gran protagonismo en el Internet del Futuro [117]. En lugar de actuar contra la congestión en puntos sobrecargados de forma individual, la actuación de forma global resulta más eficaz. Como consecuencia de esta redistribución del tráfico siguiendo el mismo criterio de equidad para otros flujos, el uso de MPTCP conduce a una mejor asignación de recursos, lo que lleva a un reparto más justo y equitativo de los recursos de la red entre los flujos de la misma, notándose su efecto en los flujos/tráfico que comparten recursos de red con la conexión MPTCP. De la misma manera, la utilización de los recursos de red sería más eficiente debido a un reparto más adecuado (lo que mejora el rendimiento de la propia conexión así como de la red de manera global) y a otras ventajas que aporta el control de congestión MPTCP, como la capacidad de acomodar picos de tráfico y un enrutamiento más optimizado y más consciente de la congestión.

Se ha de destacar que DAIMD inaugura una nueva familia de algoritmos de control de congestión en MPTCP distinta a las familias existentes de control de congestión por pérdidas y por análisis de tiempos. El mecanismo utilizado podría exportarse y aplicarse también en otros algoritmos MPTCP, como OLIA y BALIA, creando nuevos algoritmos dentro de esta nueva familia de algoritmos híbridos que presumiblemente favorecerían un reparto de recursos global más justo en la red, minimizarían las pérdidas y reducirían el tiempo total de transmisión (al mejorar en principio estos aspectos en el algoritmo en que se ha aplicado la modificación).

Por las razones expuestas anteriormente, MPTCP y en especial su control de congestión pueden utilizarse para solucionar, o al menos aliviar, el problema del tráfico creciente en redes, en el sentido de que permite la optimización del uso de las redes y la disminución de la congestión global y local.

Como protocolo de transporte es un habilitador de la interoperabilidad técnica para la comunicación de dispositivos, plataformas, aplicaciones, y otras entidades y elementos conectados a través de la red.

La interoperabilidad técnica implica la capacidad de comunicación entre dos dispositivos en la red, que podrían ser objetos inteligentes, servidores en los que rueda una plataforma IoT o una aplicación que requiere datos de sensores. Multipath TCP permite la habilitación de interoperabilidad técnica en la Internet de las Cosas generalmente conectando teléfonos inteligentes, tabletas, pasarelas IoT y servidores físicos o en la nube donde ruedan aplicaciones y servicios que usan datos IoT o plataformas IoT de gestión.

MPTCP y muy especialmente su control de congestión, mejora la capacidad para proporcionar interoperabilidad técnica de la red mediante su utilización en ella, y así como también mejora la de TCP. Por un lado permite optimizar la capacidad de las redes, y por tanto permitir un mejor rendimiento, mejorar la velocidad, y liberar recursos. Desde el punto de vista de la interoperabilidad técnica hay que destacar que además de mejorar y la calidad de servicio en la red, minimizando riesgos de congestión y colapso en la red, el CC tiene la capacidad de mantener una conexión aún ante el cierre de caminos, preservando la comunicación y la interoperabilidad técnica de esa conexión en particular.

Desde el punto de vista de la digitalización del mundo, MPTCP y DAIMD al permitir mayor eficiencia y uso de las redes actuales y nuevas redes 5G y 6G, y permitir y mejorar la interoperabilidad técnica, se les puede considerar habilitadores digitales que facilitan la transformación digital de cualquier área nuestro mundo, ya no solo permitiendo el uso de las redes de comunicación con este fin, sino mejorando la capacidad de digitalización actual con sus novedosas técnicas de mejora del rendimiento de redes y conexiones.

Por todas estas razones, se considera a MPTCP, debido a su control de congestión, una pieza clave en el Internet del Futuro, y en la que DAIMD podría ser una aportación muy valiosa y jugar un papel relevante.

Capítulo 4

Interoperabilidad basada en el uso de estándares: aplicación en el área AAL

"La comprensión mutua sería enormemente facilitada por el uso de una lengua universal"

Nikola Tesla

4.1. Introducción

La interoperabilidad en su nivel más alto (es decir, interoperabilidad semántica), requiere de la comprensión completa del significado de la información recibida entre sistemas diferentes de manera automática y no ambigua [118][7]. Como ya se mencionó en la introducción, una de las formas de habilitación de la interoperabilidad semántica entre sistemas IoT se consigue mediante la adopción de estándares de información y comunicación comunes entre esos sistemas.

Actualmente hay pocas iniciativas estandarizadas que aborden y den soluciones al reto técnico de la integración de sensores heterogéneos y sus datos (incluyendo su gestión, almacenamiento y acceso), remediando este problema la interoperabilidad. Hay que tener en cuenta que la gestión de datos incluye aspectos que engloban grandes retos técnicos como el tratamiento de datos masivos, su almacenamiento y su procesamiento en tiempo real, ya que los sistemas IoT generan datos masivos en

tiempo real (IoT Big Data) [13]. También para permitir una adecuada gestión de datos debe proporcionarse un soporte adecuado para el tipo de información manejada en IoT, como información geoespacial de movilidad asociada a las mediciones efectuadas por dispositivos inteligentes.

Una de estas iniciativas es el marco de Habilitación de servicios Web de Sensores (Sensor Web Enablement o SWE) [119] del Consorcio Geoespacial Abierto (Open Geospatial Consortium o OGC), que permite la integración de los sensores y los datos generados por ellos. Esta iniciativa en particular recibe una considerable atención en la actualidad por parte de la comunidad científica y grupos de desarrolladores. Dentro de la especificación SWE, el Servicio de Observación de Sensores (SOS) desempeña un papel muy importante en esta integración al definir una interfaz de servicio web estandarizada para acceder a los datos y metadatos de los sensores [120].

Uno de los objetivos de investigación propuestos en esta tesis es el estudio, implementación y validación de habilitadores digitales para permitir interoperabilidad entre sistemas en IoT basados en el uso de estándares. Para alcanzar este objetivo, se propone el diseño e implantación de un sistema IoT no propietario, validado en el ámbito AAL.

En concreto, en el marco de esta tesis doctoral, integrada dentro del proyecto SAFE-ECH del programa estatal I+D RETOS, se ha llevado a cabo la creación de un innovador sistema de código abierto para la gestión inteligente de residencias que realiza una implementación propia de SOS y está basado en estándares abiertos. Este sistema, SAFE-ECH, permite la integración de redes de sensores IoT heterogéneos instalados dentro de residencias, para permitir su monitorización y gestión inteligente, e implementa estándares del OGC.

Los objetivos de diseño marcados son tales que, mediante el uso de estándares abiertos y la implementación de un Servicio de Observación de Sensores, este sistema IoT:

- permita la inclusión de sensores de muy distinta tipología (en términos de magnitudes, formas de medidas y tecnologías de comunicación), permitiendo el establecimiento de interoperabilidad técnica de dispositivos en el sistema, y actuando en este sentido como una plataforma IoT integrando sensores y sus datos (integración a nivel de middleware).

- facilite la interoperabilidad sintáctica y semántica de la información mediante el seguimiento de estándares comunes, de un formato de datos concreto y proporcionando un modelo de la información (codificación y estructura). Esta interoperabilidad comprendería el ámbito del propio sistema o entre otros sistemas que utilicen esta referencia (como por ejemplo, otras instancias del sistema SAFE-ECH en otras residencias, o entidades externas que utilicen estos estándares).

Además, este sistema flexible debe permitir la gestión de múltiples residencias desde una sola instancia, creando un sistema de sistemas, siendo que cada residencia y su sistema de gestión puede considerarse un macrosistema IoT. Por tanto abordará la interoperabilidad entre sistemas dentro de un sistema-de-sistemas.

Hay que considerar que las dificultades para la habilitación de la interoperabilidad técnica de dispositivos son características en IoT y nada triviales a la hora de abordarlas, debido a la gran heterogeneidad existente a todos los niveles y a la falta de un sistema de estándares global lo suficientemente completo y actual, aceptado como estándar de facto (cuya existencia posiblemente no sea factible).

En ese sentido, los sistemas IoT de gestión son típicamente propietarios, aplican sus propios estándares cerrados y propietarios, y presentan el problema denominado "vendor lock-in" que imposibilita la inclusión de dispositivos IoT de otro fabricante. Esto, por supuesto, limita y restringe considerablemente las posibilidades de expansión del sistema y libre diseño y configuración del sistema y la red de sensores y actuadores en su conjunto: no se pueden integrar nuevos tipos de sensores que podrían ser más adecuados para determinados casos de usos y aplicación, ni elegir libremente el diseño de la red de sensores y actuadores.

Por otra parte, desde el punto de vista de la información, el uso de estándares y un modelo de información común para su representación facilita la interoperabilidad sintáctica (formato de información) y semántica (entendimiento completo y exacto de la información) dentro de un mismo sistema IoT y entre distintos sistemas que adopten como referencia este modelo. El SOS aporta un modelo lógico de información diseñado específicamente para dar soporte a información IoT de cualquier tipo de fuente, incluyendo información de geoposicionamiento y otras características específicas de datos IoT. Hay que destacar que un diseño adecuado de un modelo genérico para la representación de la información del ámbito de IoT (dispositivos y

observaciones) no es trivial. Este modelo está basado en estándares abiertos, y se apoya en el uso de elementos semánticos (marco semántico) recogidos en ontologías, permitiendo un entendimiento no ambiguo del significado de la información recogida/representada. Esta interoperabilidad de la información dependería de la adopción o correcta consulta de la referencia del modelo sintáctico y semántico por parte de sistemas o entidades externas, es decir, dependería de la adhesión a estándares de información, siendo esto una solución para la interoperabilidad semántica basada en el uso de estándares. Hay que destacar que los estándares del OGC en el marco del SWE dan un soporte apropiado a los datos IoT referentes a la información sobre sensores, independientemente de su tipología, tecnologías o la topología de la red de sensores sobre las medidas recogidas por estos, son ampliamente conocidos y reconocidos, y tienen un gran apoyo, atención y adopción en el ámbito de IoT por parte de la comunidad científica y la comunidad de desarrolladores.

En contraste, los sistemas propietarios proporcionan un modelo de información cerrado y de diseño generalmente muy heterogéneo y dispar, difícilmente adaptable y exportable a otros sistemas, sin típicamente un marco común para los distintos tipos de información gestionada, y sin soporte para nuevos o ciertas características IoT. Este modelo propietario no es entendible por otros sistemas de manera automática y no ambigua y generalmente no tiene referencias externas disponibles para su entendimiento.

El SOS, junto el marco de estándares SWE asociados, es potencialmente un habilitador digital de interoperabilidad en IoT. En primer lugar, al permitir la integración de sensores heterogéneos en un sistema IoT independientemente de sus tecnologías de comunicación, fabricante y tipología. Y, en segundo lugar, al facilitar la inteligibilidad de la información proporcionada por estos sensores dentro de un modelo de información sintáctico y semántico, ampliamente documentado, proporcionando una estructura y codificación a la información, especialmente diseñados para soportar información IoT, y con la opción de uso de soporte de ontologías para la no ambigüedad de los conceptos . adoptado. en sistemas que adoptan este estándar.

También es importante notar desde el punto de vista de la interoperabilidad que el SOS puede ser considerado como un elemento middleware que permite la interconexión e interoperabilidad de diferentes fuentes IoT (sensores, actuadores y otros dispositivos inteligentes) heterogéneas y que usan distintas tecnologías de

comunicación (ZigBee, LoRA, etc..). Es decir, el SOS se podría considerar conceptualmente desde el punto de la funcionalidad middleware equivalente a una plataforma IoT basada en estándares abiertos consolidados.

Este sistema está dirigido específicamente al área AAL de gestión de residencias, teniendo como objetivo mejorar el servicio proporcionado a los residentes, mejorando su confort, seguridad y calidad de vida, así como la optimización de procesos de gestión y funcionamiento de la residencia.

En el marco de esta investigación no se han encontrado referencias previas sobre un sistema IoT anterior en el área AAL de gestión de residencias que utilice el SOS como elemento de interoperabilidad e implemente estándares abiertos del OGC. Por tanto, se considera que constituye un enfoque innovador e inexplorado.

Este sistema ha sido implementado en diversas residencias pertenecientes al grupo SOLIMAR, permitiendo su gestión inteligente hasta la actualidad, y se prevé su inclusión futura en nuevas residencias y su posible explotación comercial.

Este sistema ha probado ser un sistema AAL funcional de gran flexibilidad para la gestión y control de residencias, siendo validado mediante su uso en residencias reales y su aplicación en muy diversos casos de uso. Ha demostrado ser capaz de incluir muy distintos tipos de sensores, y permitir la inclusión posterior de nuevos dispositivos independientemente de su tipología, magnitud en observación, método de medida, y tecnología. De la misma manera, permite la inclusión de redes de sensores de muy distinta topología compuestas por sensores heterogéneos, integrando las variaciones de la red en el tiempo (inclusión, movimiento o eliminación de dispositivos inteligentes). Es un sistema aplicable a los distintos casos de uso en residencias, facilitando la gestión y los procesos y flexible para la adopción de múltiples casos de uso de gestión de residencia apoyados en tecnologías IoT.

Fuera del ámbito de gestión de residencias, se podría implementar en sistemas IoT que decidan adoptar los estándares OGC para la gestión de sus datos, y opten por su uso para proporcionar una gestión inteligente de la información IoT recogida. Para ello sería necesario una adaptación de los servicios proporcionados. Se estudia su inclusión futura en Hogares Inteligentes (especialmente en los orientados al cuidado y seguridad de la tercera edad) y en hospitales.

4.2. ESTADO DEL ARTE

4.2.1. AAL, AMI e IOT

Una de las áreas donde más beneficios pueden obtenerse de la aplicación de IoT y de la interoperabilidad asociada a sistemas IoT y su información es el sector de la salud y los entornos inteligentes para el cuidado de personas [121]. Los dispositivos IoT permiten la monitorización remota en tiempo real y en todo momento de constantes vitales, medidas y eventos en entornos inteligentes sensorizados de importancia para el cuidado y el bienestar de las personas, detectando y alertando inmediatamente de situaciones que requieran atención, y permitiendo una monitorización precisa y constante de muchos factores y aspectos importantes, y un posterior análisis inteligente de estos datos. El paradigma de cuidado clásico no puede llegar al alcance y a las posibilidades que permiten los sistemas IoT, siendo sus beneficios potenciales y posibilidades de uso muy significativamente mayores.

Por ello, IoT puede mejorar drásticamente la calidad de vida de la población de edad avanzada. En este sentido, los Entornos Inteligentes (AMI) [122] de Vida Asistida (AAL) [123] y el Envejecimiento Activo y Saludable (AHA) [124] son campos con un enorme potencial para beneficiarse del uso de sistemas IoT.

Los Entornos Ambientales Inteligentes (AMI) [125] son entornos sensibles a la presencia y actividad de las personas y que responden de manera inteligente a los estímulos e información recibida con acciones específicas. Por otro lado, los Entornos de Vida Asistida (AAL) se corresponden a una subárea de los Entonos Inteligentes (AMI) que tiene como objetivo proporcionar servicios, transparentes o no para el usuario final, orientados al cuidado y la asistencia de personas en su día a día (generalmente ancianos o pacientes). En este capítulo se estudiará un caso práctico de aplicación de tecnología IoT para la creación de un sistema AAL en residencias de ancianos, con el objetivo de mejorar su bienestar, seguridad y calidad de vida.

4.2.2. Marco de estandarización SWE

4.2.2.1 *Necesidad de la Web de Sensores (SWE)*

La inteligencia ambiental requiere el uso de redes de sensores para recoger información del entorno de forma transparente para el usuario final. Sin embargo,

esa transparencia esconde una complejidad inherente a muchos niveles. Las redes de sensores en IoT suelen presentar una gran heterogeneidad: los sensores tienen diferentes especificaciones, proveedores y patrones de medición. Además, los sensores pueden presentar movilidad y no estar situados en una posición espacial fija. Los datos recogidos por los objetos inteligentes se transmiten a través de tecnologías y protocolos muy diversos, como: Wi-Fi [126], Bluetooth [127], Zig-bee [128], 6LowPAN [129], UDP [130], LoRa [131], TCP [110], MQTT [132], etc. La integración de los sensores y sus datos no es una cuestión trivial debido a esta heterogeneidad, y lo mismo ocurre con el acceso y la gestión de estos datos [11][12]. La cantidad masiva de datos que generan las redes de sensores IoT requiere (adicionalmente) un almacenamiento masivo, normalmente ubicado en la nube [13][14], junto con la necesidad de recuperarlos y gestionarlos. Esto representa un reto añadido para los sistemas IoT.

Hay pocas iniciativas estandarizadas que aborden y den soluciones a este problema de interoperabilidad. Una de ellas que recibe una atención considerable desde la comunidad científica y de desarrolladores es el marco Sensor Web Enablement (SWE) [133] del Open Geospatial Consortium (OGC) [134], que permite la integración de los sensores y los datos generados por ellos. En particular, el Servicio de Observación de Sensores (SOS) [135], que forma parte de la especificación SWE, desempeña un papel importante en esta integración al definir una interfaz para acceder a los datos y metadatos de los sensores [136]. El SOS proporciona una interfaz de servicio web estandarizada que permite a los clientes interactuar con los sensores registrados y sus mediciones [120], y también registrar nuevos sensores y observaciones, o eliminarlos.

La movilidad es una característica clave del IoT [137][138][139]. Incluso en los sensores fijos, la posición espacial de un objeto inteligente puede ser relevante en el análisis de los datos del sensor. Muchos sensores son objetos móviles, y esta característica permite un seguimiento diferente de los aspectos del entorno, que de otro modo no puede abordarse con sensores fijos. Los teléfonos móviles son un claro ejemplo de la presencia masiva de objetos inteligentes móviles en la IoT. Los aspectos de la movilidad en objetos inteligentes deben ser abordados para poder permitir la itinerancia entre diferentes redes, y para entender de una manera más completa la información de monitorización que proporcionan. Las redes móviles de sensores en entornos especiales pueden incluso requerir el uso de pasarelas móviles [140] [60]; en este tipo de sistemas de IoT la información de posición de la pasarela y el sensor

es crucial para el funcionamiento del sistema y el análisis de los datos de monitorización. Los aspectos relacionados con la movilidad pueden ser especialmente útiles e interesantes para AAL, ya que la información sobre la ubicación y el seguimiento son potencialmente de gran utilidad para muchos servicios dentro de, por ejemplo, una residencia de ancianos o en los hogares inteligentes para personas mayores. El uso de metadatos geoespaciales puede resolver los retos anteriormente mencionados (itinerancia en redes, necesidad de soporte geoespacial, explotación de información geoespacial). En este sentido, el OGC proporciona estándares que soportan la geolocalización de los sensores y las mediciones de los mismos [135]. Esta característica de gran relevancia para la IoT, sin embargo, no está presente en muchos modelos de información [141], siendo el soporte a la información de posicionamiento o movilidad una necesidad de los modelos de información para IoT [139][142].

4.2.2.2 *Paradigma OGC de la Web de Sensores (SWE)*

Sensor Web Enablement (SWE) [143] es un marco y un conjunto de estándares del OGC que permiten la explotación de sensores y conjuntos de sensores conectados a una red de comunicación. SWE se basa en el concepto de Sensor Web: “las redes de sensores accesibles a través de la web y los datos recogidos y enviados por estos sensores, que pueden ser descubiertos y accedidos usando protocolos estándar e Interfaces de Programa de Aplicación (APIs)" [135][134]. Su objetivo es hacer accesibles todo tipo de sensores y datos de sensores mediante el uso de protocolos estándar e interfaces de aplicación, a través del uso de protocolos de Internet Web y el lenguaje XML (o su formalismo equivalente usando estructuras JSON). De este modo, se puede publicar las características de los sensores, como sus interfaces, su capacidad y su posición. Esta información puede ser utilizada por las aplicaciones para geolocalizar y procesar los datos recogidos por el sensor sin necesidad de conocer previamente el sistema del mismo. El SWE es un grupo de especificaciones que abarcan sensores, modelos de datos relacionados y servicios que ofrecen accesibilidad y control a través de la Web. La arquitectura del SWE se compone de dos modelos principales: el modelo de información y el modelo de servicio [144]. El modelo de información describe los modelos conceptuales y las codificaciones utilizadas para implementarlos, mientras que el modelo de servicio precisa las especificaciones de los servicios asociados. En el modelo de información, los modelos conceptuales son: transductores, procesos, sistemas y observaciones. Las codificaciones son: Observations & Measurements Schema (O&M) [145][146], Sensor

Model Language (SensorML) [136][147] y Transducer Markup Language (TransducerML o TML) [144].

El modelo de servicio describe los servicios dentro del marco SWE que permiten a las aplicaciones acceder de forma interoperable a la información de los sensores y realizar operaciones de gestión sobre ella. El modelo de servicios de SWE incluye especificaciones para cinco servicios: Servicio de Observación de Sensores (SOS) [135], Servicio de Alerta de Sensores (SAS) [148], Servicio de Planificación de Sensores (SPS) [], Servicios de Notificación Web (WNS) y Servicio de Catálogo Web (CSW) [28]. A continuación se describen los servicios SOS y SAS, los cuales tienen especial relevancia en el capítulo.

Servicio de Observación de Sensores

El Servicio de Observación de Sensores (SOS) es una parte del marco SWE que define un modelo común para todos los sensores, sistemas de sensores y sus observaciones. El modelo es horizontal, ya que puede aplicarse en cualquier dominio de IoT, y es independiente de aplicaciones específicas [149]. En este sentido el SOS es un elemento que, proporcionando este modelo, hace de intermediario entre un cliente y un repositorio de observaciones o una red de sensores casi en tiempo real. Los clientes, además de poder acceder a los datos de las observaciones de sensores, también pueden acceder al SOS para obtener información de metadatos que describen a los sensores asociados, las plataformas, los procedimientos, o bien de otros metadatos asociados a las observaciones [150][151].

La versión más reciente de SOS es la 2.0 [135] que, entre otras actualizaciones, permite el uso tanto de mensajes JSON como XML y cuatro perfiles de operaciones (Core, Transactional, Enhanced y Result Handling).

Se han desarrollado varias implementaciones del SOS. La más completa y mayormente utilizada es el 52°North SOS [152]. Bajo la licencia GPL (GNU Licencia Pública General), el 52°North SOS está implementado en Java, por lo que es agnóstico a la plataforma (puede ejecutarse en cualquier sistema operativo), y soporta todos los perfiles operativos del SOS. Ofrece una amplia documentación en línea y recibe el apoyo constante de una comunidad activa y numerosa. Esta implementación concreta del SOS forma parte de un conjunto de implementaciones de servicios web de sensores de la comunidad 52°North [153][154][155]. Otras implementaciones son PySOS [156], MapServer SOS [157], y Deegree SOS [158]. PySOS es la única

implementación basada en Python del estándar OGC SOS, desarrollada por la comunidad de investigación oceánica. Todas estas implementaciones ofrecen una funcionalidad limitada y no tienen soporte actual.

Las implementaciones del SOS suelen requerir considerables recursos computacionales ya que generalmente están diseñadas para poder cubrir las necesidades de cualquier escenario factible. Cambiando este planteamiento para priorizar la optimización de recursos y siguiendo las recomendaciones del OGC para la creación de un SOS para sensores fijos [135][134] SOSLite [159][160] es una implementación ligera del SOS.

Servicio de Alerta de Sensores

El Servicio de Alertas de Sensores (SAS) [148]: es un servicio de notificación de eventos basado en el patrón de publicación y suscripción. Un Productor puede incluir y configurar eventos, y el Consumidor puede suscribirse a ellos para ser notificado automáticamente cada vez que el evento ocurra.

4.3. Sistema SAFE-ECH

En el marco del proyecto RETOS "SAFE-ECH" [161] y de la investigación realizada en esta tesis doctoral se ha diseñado el sistema SAFE-ECH [158][122], un sistema inteligente de AAL basado en código abierto para la monitorización de residencias de ancianos, con el objetivo de cubrir necesidades AAL y AMI en residencias, mejorar la calidad de vida de sus usuarios y proporcionar un sistema alternativo a los distintos software de gestión propietarios que se utilizan de manera local y dispar, aportando un sistema flexible, de gran usabilidad y basado en código abierto que permite la conexión e interoperabilidad de dispositivos IoT, independientemente de su marca y características, y que facilita la interoperabilidad semántica de su información aplicando estándares OGC/SWE, así como el análisis inteligente de esta información. Además, también habilita la posibilidad la integración e interoperación de múltiples residencias estableciendo un sistema de sistemas IoT.

SAFE-ECH apoya el Envejecimiento Activo y Saludable (AHA) [162][163], y tiene como objetivo atender las necesidades de las personas mayores en las residencias, proporcionando servicios para mejorar su calidad de vida, la atención sanitaria, la seguridad, la movilidad y el confort, entre otros aspectos.

Este sistema AAL tiene como objetivo central mejorar la calidad de vida de las personas mayores que viven en residencias. La tecnología IoT tiene un enorme potencial para mejorar de forma significativa la eficacia de los servicios de atención a los ancianos y optimizar las condiciones ambientales de una residencia mediante la creación de un entorno de Inteligencia Ambiental de Vida Asistida [164][165]. En este sentido, SAFE-ECH crea un entorno inteligente en una residencia mediante la recopilación y el almacenamiento de datos de monitorización de sensores IoT desplegados en ella, la realización de un análisis inteligente de los datos y, en respuesta a los resultados de este análisis, la aplicación de ciertas acciones específicas para mejorar la seguridad, la comodidad y el cuidado eficiente de las personas mayores. Además, este sistema expone una interfaz hombre-máquina (HMI) que permite su configuración, y que facilita su trabajo a trabajadores de la residencia (cuidadores, médicos, gestores) al permitirles acceder a la información de monitorización de esta, dispuesta de forma amigable y visual, recibir notificaciones y alarmas, configurar el sistema y realizar acciones de control. De esta manera los cuidadores pueden efectuar de forma más eficiente su trabajo, con un mayor control de la situación global de la residencia y conocimiento de alertas y eventos que afectan o pueden afectar a los residentes, además de recibir ayuda automática de forma transparente con ciertos procesos y servicios (como la regulación automática de luminarias o aire acondicionado, o la gestión automática del control de acceso al recinto y las habitaciones). Notablemente, todo este control inteligente puede incluso permitir su proactividad previniendo situaciones potenciales de peligro que no habrían podido detectarse anticipadamente sin la ayuda de dispositivos IoT y el análisis inteligente de la información recogida.

Este sistema se adapta a las necesidades específicas de cada residencia, integrando los sensores, actuadores, reglas y servicios necesarios. Es escalable y permite la gestión de varias residencias simultáneamente.

Como elementos innovadores, integra y hace uso de un Servicio de Observación de Sensores del marco SWE y utiliza estándares abiertos del OGC. Además, emplea un procesador de eventos complejos (CEP) [166] para dotar de inteligencia al sistema, efectuando un análisis inteligente de los datos y proporcionando respuestas inteligentes a combinaciones no triviales de eventos que pueden ser difíciles de detectar (eventos complejos). Dentro de nuestro conocimiento, no se ha publicado información de ningún sistema anterior con estas características, es decir, sobre un

sistema AAL para la gestión inteligente de residencias haciendo uso de un Servicio de Observación de Sensores y estándares abiertos.

Desde un punto de vista de gestión e integración de los datos y la información, este sistema se basa en estándares abiertos y sigue el marco Sensor Web Enablement (SWE) [119] del Open Geospatial Consortium (OGC) cumpliendo con las especificaciones Observations & Measurements Schema (O&M), SensorML y Sensor Web Enablement (SWE). Utiliza el SOS como elemento clave para la integración de sensores procedentes de redes de sensores inteligentes, y la gestión y acceso a sus medidas o información de monitorización. Por otro lado, desde el punto de vista de análisis de la información su procesador de eventos complejos permite respuestas inteligentes a combinaciones de eventos y situaciones muy específicas, creando un entorno AMI.

SAFE-ECH tiene dos modos de funcionamiento: Gestión Local, que permite la monitorización y control de una sola residencia, y Gestión de Múltiples Residencias (gestión global), que permite la monitorización de varias residencias simultáneamente. Estos dos modos presentan una gran flexibilidad, y un sistema SAFE-ECH de gestión global puede integrar varios sistemas de gestión local.

De manera práctica, este sistema se preparó para proporcionar servicios AAL y cubrir las necesidades de un conjunto de siete residencias reales. Después del periodo de pruebas, finalmente, se implementó y conectó el sistema a una residencia del grupo (residencia piloto) para evaluar el sistema, planeándose la incorporación futura de las otras seis en las que se ya se había testeado su uso en entorno de pruebas. El conjunto de residencias comprende a las siete residencias de la tercera edad del grupo SOLIMAR en las localidades de Sollana, la Valldigna, Cullera, Daimús, la Ollería, Massanassa y Alzira.

Figura 4.1 Mapa del grupo de residencias en las que se probará el sistema

Este trabajo ha sido el fruto de un proyecto colaborativo entre la Universidad Politécnica de Valencia , la empresa ISECO[1], proveedora tecnológica de residencias, y la empresa de centros para la tercera edad SOLIMAR[2].

En el marco de esta tesis se ha desarrollado directamente el sistema central y los scripts del gestor de mensajería con el asesoramiento de ISECO respecto a servicios y datos a integrar como experto tecnológico en dispositivos IoT y servicios AAL. ISECO y SOLIMAR, como expertos en gestión de residencias aportaron conocimientos e información en lo referente a requerimientos, casos de uso y servicios. Se ha colaborado muy estrechamente con ISECO quien ha desarrollado, implementado e instalado los sistemas de adquisición y actuación dentro de las residencias. Algunas tareas puntuales en estas dos áreas de trabajo (sistema central y sistema de adquisición de datos y actuación) se han hecho colaborativa y conjuntamente.

4.3.1. Objetivos de diseño

El proyecto tiene como meta acceder al mercado socio-sanitario (en particular en el área de residencias de la tercera edad) donde haga falta una solución no propietaria con sensores de distinta naturaleza y tipología, y desarrollar de un nuevo sistema de monitorización y control, basado en estándares abiertos de comunicaciones, gestión

[1] www.iseco.es

[2] www.solimar.es

de información, interoperabilidad, representación de la información y razonamiento lógico.

Para ello SAFE-ECH tiene como objetivo principal el desarrollo e implantación de un sistema de monitorización y control para la supervisión de una residencia de la tercera edad, considerando que la seguridad, salud y confort de las personas (residentes y trabajadores) es clave en el funcionamiento de la misma. Para ello pretende mejorar y automatizar los métodos actuales de gestión de la seguridad y salud, que generalmente no son integrales y suelen diseñarse de manera independiente a la del resto de la residencia y sus procesos. Hay que tener en cuenta que los diferentes sistemas de gestión desarrollados en la actualidad son en general limitados y propietarios, lo que impide en muchos casos la interoperabilidad, extensión del sistema con nuevos elementos y jerarquización. Desde el punto de vista de utilización de sistemas IoT existentes, típicamente se presentan limitaciones muy importantes en la integración de sensores por el problema denominado “vendor lock-in”, es decir, la imposibilidad de una plataforma o sistema de gestión propietario para integrar dispositivos IoT de una marca o fabricante diferente.

Desde un punto de vista técnico, los objetivos generales de diseño del sistema serían:

1.- Agregación de nuevos sensores con independencia del fabricante de los mismos, homogeneizando la información almacenada y utilizada por las herramientas de gestión.

2.- Posibilidad de incluir la información procedente de los sensores en el sistema de planificación de recursos empresariales (ERP) de la empresa de gestión.

3.- Acceso a la información desde cualquier punto con conectividad, limitando el acceso al HMI en función del grado de privacidad requerido, así como los privilegios por parte del usuario.

4.- Extensión jerárquica del sistema permitiendo una monitorización y gestión centralizada de varias residencias de un mismo grupo sin ninguna modificación en la operación del sistema.

5.- Gestión segura de la información según los procedimientos y normas que afectan al tratamiento de la información médica y de seguimiento teniendo en cuenta siempre la privacidad y dignidad de las personas.

6.- Mecanismos de razonamiento personalizados para la operación de la residencia en el ámbito de los residentes y trabajadores, teniendo en cuenta factores como por ejemplo el historial médico o la medicación aplicada, o bien mecanismos más generalizados para la gestión de la propia residencia como un edificio inteligente.

7. Gestión de la información de geoposicionamiento dentro la información de monitorización de los sensores IoT, incluida en datos o metadatos.

8. Uso de estándares abiertos ampliamente aceptados y adoptados

9. Gestión de alarmas y eventos en la residencia

10. Proporcionar un sistema del gran usabilidad a trabajadores y gestores, que permita visualizar la información clave de monitorización de una residencia en tiempo real (incluyendo alertas y alarmas), así como acceder a históricos de información

La mayor parte de estos objetivos (1,2,3,4, 8 e indirectamente los objetivos de gestión) están relacionados con la interoperabilidad, ya sea inter-sistema o intra-sistema.

Basándose en estos objetivos y en otros puntos importantes en el diseño de la solución se identificó una larga lista de requerimientos técnicos, especificados en el entregable D1.2 del proyecto, a partir de los cuales se definió la arquitectura y se desarrolló el software del sistema.

4.4. Usuarios del sistema

En el entorno de la residencia se han diferenciado distintos tipos de actores o perfiles de usuario, que interactúan de manera diferente con el sistema AAL SAFE-ECH y el entorno inteligente generado:

1. **Residentes**: usuarios finales que se benefician de los aportes del sistema SAFE-ECH a las mejoras de servicio y asistencia en la residencia. No tienen acceso al sistema de control y monitorización, que es transparente para ellos. Tienen la capacidad de activar alarmas (tiradores de emergencia) y de comunicarse con el puesto de control de la residencia a voluntad. Cierto tipo de actividad por su parte pueden ser detectada y registrada por la red de dispositivos inteligentes de la residencia.

2. **Cuidadores**: trabajadores de la residencia que proporcionan cuidados y atención a los residentes, y efectúan diversas tareas esenciales para el funcionamiento de la residencia. Entre ellos se incluye el servicio médico de la residencia, enfermeros, sanitarios y cuidadores habilitados. Tienen acceso al sistema SAFE-ECH a través de su interfaz de monitorización de residencia (HMI). En general no tienen asignados permisos para cambiar la configuración del sistema, refiriéndose a las órdenes de control programadas o a las reglas de análisis inteligente por las cuales cierta secuencia de eventos desencadena una determinada acción. No tienen conocimientos técnicos informáticos, por lo que la interfaz HMI debe tener un GUI y alta usabilidad, y proporcionar información lo suficientemente accesible.
3. **Gestores del puesto de control**: trabajador que actúa desde el puesto de control de la residencia, monitorizando el funcionamiento de la residencia y tomando decisiones de control. Tienen permisos de configuración del sistema, pudiendo establecer reglas lógicas de funcionamiento ante determinados estímulos y ejecutar órdenes de control. Generalmente tienen conocimientos informáticos básicos.
4. **Gestor de sistemas**: trabajador con conocimientos informáticos que se encarga de la instalación de programas y gestión informática de equipos.
5. **Familiares o visitantes**: personas que pueden estar dentro del recinto de la residencia visitando a los residentes y que no presentan apenas interactuación con el sistema.

De entre todos los usuarios identificados solo los trabajadores (cuidadores y gestores) tendrán acceso al sistema SAFE-ECH. Desde un punto de vista de gestión de usuarios existirán diferentes niveles de permisos para ellos respecto a su interacción con HMI. Solo los usuarios gestores con permisos elevados podrán editar las reglas de gestión de la residencia y tener acceso a ciertos registros. Los trabajadores con un permiso de gestión menor podrán visualizar la configuración y las reglas establecidas, pero no cambiarlas, y siempre tendrán acceso a la información de monitorización, eventos y alarmas generadas (en tiempo real o en históricos).

4.5. Casos de uso y servicios

El sistema debe integrar distintos casos de uso proporcionando diferentes servicios AAL en residencias. Se han identificado y diseñado los siguientes casos de uso, enmarcando cada uno un servicio asociado:

- **Iluminación inteligente:** permite el control automático sin intervención humana de luminarias de la residencia dependiendo de las condiciones lumínicas o el horario.
- **Control de errantes**: control de acceso y registro de localización de residentes desorientados o "errantes", como por ejemplo ancianos con casos graves de Alzheimer, que por su propia seguridad deben tener restringido el acceso a ciertas áreas. Los intentos fallidos de acceso a zonas no restringidas deben ser alertados. Así mismo las restricciones de acceso deben presentar excepciones cuando se encuentran acompañados por trabajadores del centro o familiares, autorizados para estar a su cargo, en determinadas franjas horarias.
- **Control de accesos:** por razones de privacidad y seguridad los accesos a las habitaciones de los residentes, otras zonas de la residencia y exteriores deben estar restringido a solo usuarios autorizados, y mediante el uso de la tecnología, este control debe ser automático y registrar intentos fallidos de entrada a zonas no permitidas.
- **Detección de intrusos y cierre perimetral**: las zonas de posible entrada a la residencia (perímetro) deben estar debidamente protegidas frente a accesos no permitidos, y disparar una alerta en caso de entrada no autorizada fallida o exitosa. El cierre perimetral de puertas por sistema magnético permite su cierre automático en determinadas franjas de tiempo y determinados sensores pueden detectar intentos fallidos de entrada y provocar alarmas.
- **Detección de incendios/humos:** permite monitorizar que en todo el recinto de la residencia la existencia o no de concentraciones de CO2 que puedan indicar la presencia de humo, y alertar ante su presencia para prevenir una posible situación de incendio.
- **Alarma médica (emergencia vital):** en caso de requerir atención y asistencia inmediata, los residentes pueden activar esta alarma pulsando botones de pánico o tiradores de emergencia a su alcance. También podría activarse ante determinados registros de otro tipo de sensores (en general sensores médicos). Este caso de uso requiere de un protocolo asociado de gestión,

atención y desactivación por parte de los trabajadores prestando asistencia para garantizar la máxima rapidez y eficacia.

- **Comunicaciones con el centro de control:** servicio disponible para residentes a través de un terminal de comunicaciones
- **Regulación inteligente del aire acondicionado (frío y calor):** permite el control automático de la temperatura de habitaciones y zonas comunes para garantizar condiciones de temperatura óptimas dentro de la residencia a los ancianos, garantizando su confort y bienestar.
- **Registro de actuaciones de los trabajadores:** distintas acciones realizadas por trabajadores deben poder registrarse al momento de su realización para un mejor control y gestión de las tareas de la residencia, y proporcionar la mejor atención posible a residentes. Comprendería tareas como hacer la cama, bañar a un residente, limpiar la habitación, cambiar pañales, asistir una emergencia avisada por la alarma médica, etc. y requeriría como mínimo indicar la acción, id de trabajador e id de plaza de residente.
- **Eliminación de sujeciones de seguridad y mantenimiento del control y seguridad mediante sensorización de presencia o presión.** En el cuidado tradicional a algunos residentes, por su propia seguridad, se les sujetaba en la cama. Esto puede ser sustituido por sensores específicos de presión o presencia que permiten alertar en caso de emergencia.
- **Control de pañales:** el uso de dispositivos de detección de humedad permite una mayor eficiencia en las tareas de control de pañales, pudiendo los trabajadores saber sin tener que molestar al residente la necesidad de un cambio, siendo alertados inmediata y remotamente de la necesidad de cambio. Desde un punto de vista sanitario y de bienestar del residente, esta aplicación de la tecnología frente al cuidado clásico presenta ventajas altísimamente significativas**.** Con el sistema tradicional de comprobación por turnos diarios se molesta innecesariamente al residente, se consume mucho tiempo en comprobaciones innecesarias, y el tiempo de cambiado de pañales no es el óptimo, pudiendo estar el residente mucho tiempo en espera necesitándolo.

Estos casos de uso serán empleados en el grupo de residencias SOLIMAR, pudiendo cada residencia adoptar un subgrupo de ellos (o todo el conjunto) según sus necesidades específicas.

En concreto, en la residencia piloto se planeó el despliegue de los servicios de Iluminación Inteligente, Detección de Incendios, Control de Accesos, Emergencia Vital (alarma médica), Cierre Perimetral y Actuaciones de Trabajadores.

El control y monitorización de las residencias requiere del uso de dispositivos inteligentes capaces de recoger información clave del entorno o de los usuarios para garantizar y poder crear un entorno inteligente. Es por ello necesaria la sensorización de la residencia que utilice el sistema, desplegando sensores y actuadores IoT que permiten los servicios AAL asociados a estos casos de uso. Así pues, estos casos de uso estarán apoyados por el uso de dispositivos inteligentes IoT (sensores y actuadores) desplegados en la residencia:

- Sensor de humos
- Tirador de emergencia o botón de pánico
- Terminal de comunicaciones
- Sensor de temperatura
- Dispositivo de control de acceso
- Cierre magnético de puertas
- Sensor de presión (variantes cama, silla y suelo)
- Sensor de iluminación
- Sensor de enuresis
- Pulsera de localización
- Móviles
- Actuador del aire acondicionado
- Actuador del sistema de iluminación

Estos sensores y actuadores deben ser desplegados en las habitaciones de los residentes y en las zonas comunes. Es necesario garantizar la conectividad, tanto inalámbrica como cableada, en toda la residencia para permitir la conexión de estos dispositivos inteligentes a su red o redes locales (LAN). Así mismo desde esta red local se deberá tener capacidad de conexión y acceso al servidor del sistema central de gestión donde se deberá recibir y gestionar la información recogida por los sensores.

Además, para la ejecución de muchos casos de uso es necesario contar con la inteligencia del sistema, que en respuesta a diferentes eventos y situaciones debe actuar avisando a trabajadores o ejecutando ciertas órdenes de control.

4.6. Arquitectura del sistema

Tras la fase de preparación del diseño del sistema (identificación y análisis de requisitos y especificación funcional) se diseñó la arquitectura del sistema de monitorización, descrita en los siguientes apartados. En primer lugar se describe como una visión conceptual de alto nivel, dividendo la solución en diferentes niveles o capas. En segundo lugar se describe la arquitectura en mayor detalle desde una perspectiva orientada a servicios (SOA), y finalmente desde una perspectiva de componente. Algunas capas, componentes o características clave del sistema son vistas en detalle en las últimas subsecciones.

4.6.1. Esquema conceptual de la arquitectura a alto nivel

Desde una visión conceptual a alto nivel, la arquitectura de la solución propuesta contaría con tres bloques principales y dos capas transversales, como puede verse en la Figura 4.2.

Figura 4.2 Esquema de capas y niveles de la arquitectura del sistema

La arquitectura de SAFE-ECH está compuesta por los siguientes bloques principales:

- **Nivel de Adquisición y Actuación**, referente a la capa compuesta por sensores y actuadores desplegados en la residencia, los módulos de adquisición de

datos y actuación, y a las comunicaciones de bajo nivel, inalámbricas o cableadas.

- **Nivel de Comunicaciones**, encargado de dirigir la información de los sensores y grupos de sensores hacia el o los servidores de monitorización y control, donde reside el sistema central de SAFE-ECH, y de igual forma dirigir la información de este hacia los actuadores.
- **Servicios y Servidores en el centro de contro**l que contendrán la inteligencia y herramientas de gestión de la organización.

Además, la arquitectura de la solución SAFE-ECH cuenta con dos capas transversales a estos tres bloques:

- **La capa de Seguridad** del sistema global a nivel de comunicaciones, información y control de acceso, que protege en cuenta la naturaleza de la información gestionada, que es en algunos casos de tipo médico o de localización de las personas, lo que implica la necesidad de alta privacidad y puede ser crítica.
- **La capa de Semántica e Inteligencia** del sistema basado en la adecuada representación de la información, facilitando la interoperabilidad sintáctica y semántica de los datos, y la fijación de reglas de razonamiento lógico.

4.6.2. Visión de la arquitectura desde una perspectiva de arquitectura orientada a servicios (SOA)

El enfoque de Inteligencia Ambiental suele centrarse en los servicios e interacciones inteligentes que se proporcionan en el entorno, de forma transparente, y deja las tecnologías y componentes en otro plano inferior. Por ello, una Arquitectura Orientada a Servicios (SOA) describe de forma óptima, desde esta perspectiva, el entorno de Inteligencia Ambiental AAL que crea el sistema. Este entorno se representa como un conjunto de servicios que reciben los residentes (usuarios finales) además de los servicios que ayudan a los cuidadores a mejorar la eficiencia de su atención a los ancianos.

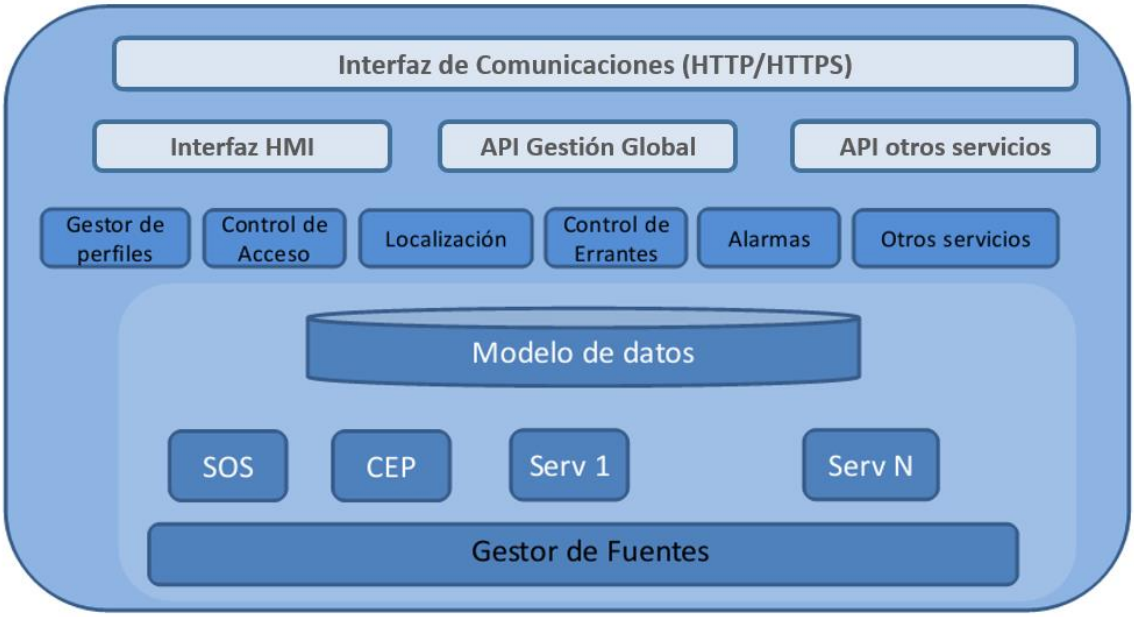


Figura 4.3 Arquitectura orientada a los servicios

Los diferentes niveles de nuestro sistema desde una perspectiva SOA pueden verse en la Figura 4.3. Siguiendo una perspectiva top-bottom, los componentes de nuestro sistema son los siguientes:

- Una interfaz de comunicación basada en el protocolo HTTP. Los agentes humanos (cuidadores y administradores) pueden acceder a los servicios del servidor a través de la interfaz HTTP proporcionada por un servicio web del sistema. Esta interfaz incorpora medidas de seguridad como autenticación y gestión de autenticidad mediante encriptación y uso de certificados.

- Más allá de la interfaz de comunicación (HTTP) el sistema cuenta con una interfaz web frontal del sistema central que permite a los cuidadores el acceso a diferentes servicios de administración:

    - HMI: Interfaz Hombre-Máquina a la que sólo pueden acceder los usuarios autorizados. Muestra información de monitorización, lanza alarmas y notificaciones, y permite realizar acciones de configuración y control del sistema en la residencia.

- API: Interfaz de programa de aplicación para la configuración, supervisión y administración de una sola residencia (Gestión local) o de múltiples residencias (Gestión global), y otros servicios.

• Los servicios finales de SAFE-ECH se encuentran en un nivel inferior del modelo SOA. Los ancianos residentes, como usuarios finales del sistema, se benefician directa e indirectamente de estos servicios AAL, diseñados para mejorar el confort y la calidad de vida de los residentes. Estos servicios permiten a los cuidadores mejorar su conocimiento de las situaciones en la residencia de ancianos que requieren su atención, así como potenciar la calidad y eficiencia del servicio de atención que prestan a los residentes. Algunos de los servicios más importantes, ya descritos en un apartado anterior, son: detección de intrusos, control de acceso, servicio de control de errantes, servicio de alarma y servicio de pañales. Otros servicios innovadores en el ámbito de AAL en las residencias de ancianos son los servicios de geolocalización. En el ámbito de AAL y AHA estos servicios son especialmente útiles. Hay que señalar que el uso de estándares OGC abiertos y el soporte de metadatos geoespaciales permiten el uso de servicios basados en el seguimiento, y la mejora de otros servicios mediante el uso de información geoespacial adicional.

El gestor de fuentes se encarga de la comunicación con los módulos externos de adquisición de datos (sensores) y de actuación. El Módulo de Adquisición de datos se encarga de proporcionar información de monitorización al Sistema Central desde la red de sensores, a través de la interfaz SOS y se almacena en la base de datos asociada a este servicio. Por otro lado, el Módulo de Actuadores se encarga de realizar las acciones y órdenes del sistema Central sobre los actuadores.

4.6.3. Definición de la arquitectura desde una perspectiva de componentes

La arquitectura del sistema desde un enfoque de bajo nivel desde una perspectiva de componentes se muestra en la Figura 4.4 y se describe en este apartado. Además, también se presenta la arquitectura de software del sistema central.

Los diferentes elementos que componen SAFE-ECH se detallan a continuación:

• **Red de sensores:** es el conjunto de sensores colocados en una residencia de ancianos con fines de monitorización para poder tener información de la situación actual y detectar eventos relevantes. Son la principal fuente de información del

sistema y permiten crear un entorno de Inteligencia Ambiental sensible en la residencia de ancianos. Su función es monitorizar la residencia de ancianos y enviar los datos generados al Módulo de Adquisición de Datos de los Sensores. Este Módulo recoge los datos de los sensores y los envía al sistema central. Los sensores y las observaciones de los sensores tienen asociados metadatos de geolocalización que siguen las especificaciones del OGC. Esta característica permite una funcionalidad adicional de movilidad y posicionamiento.

- **Sistema de actuadores:** es el conjunto de actuadores dentro de la residencia. Ejecutan las órdenes dadas desde el sistema central, que reciben a través del Módulo de Actuadores.

- **Sistema central:** el núcleo del sistema, alojado en un servidor, el cual es capaz de recoger y almacenar los datos de los sensores, analizarlos y realizar acciones específicas en caso de que su inteligencia considere que deben tener lugar en respuesta a situaciones concretas. Estas acciones pueden ser notificaciones visibles a través de la HMI, órdenes a los actuadores o el lanzamiento de alarmas. Implementa servicios específicos del marco SWE: un Servicio de Observación de Sensores y un Servicio de Alarmas de Sensores.

    - **HMI:** Interfaz hombre-máquina del sistema central a la que se puede acceder en línea a través de una interfaz web. Los usuarios autorizados pueden visualizar la información de monitorización, configurar los servicios del sistema y realizar acciones de gestión y control.

El sistema central está compuesto por otros componentes que se describen en detalle a continuación. Además, se dan las especificaciones del software del sistema central de código abierto, detallando así la arquitectura del software.

- Un **Servicio de Observación de Sensores (SOS)** como elemento responsable de la recopilación, el almacenamiento y la recuperación de los datos de los sensores. Sigue los estándares del Open Geospatial Consortium (OGC), y proporciona una interfaz estándar para gestionar y recuperar los datos y metadatos de los sensores y las observaciones de los sensores [135] [151]. Para ello, el SOS ofrece un conjunto de operaciones que los clientes de este servicio pueden utilizar independientemente de su dominio o aplicaciones asociadas. De esta forma, los datos son accedidos por otros elementos del sistema que pueden realizar análisis de datos, mostrar información de monitorización y habilitar los servicios AAL que ofrece SAFE-ECH. Permite el acceso a

cualquier sistema de sensores, ya sean in-situ, remotos, fijos o móviles, permitiendo la interoperabilidad. SOS se basa en tecnologías web ampliamente aceptadas como XML, JSON y SOAP, típicamente utilizadas en IoT. Los sensores registrados pueden introducir sus observaciones en el SOS, que las almacena en una base de datos con soporte geoespacial. El SOS cumple con la especificación "Observations & Measurements Schema" (O&M) [145][146] para modelar las observaciones de los sensores, y con la especificación Sensor Model Language (SensorML) [136] para modelar sensores y sistemas de sensores. Nuestro sistema utiliza la implementación del SOS 52º North [152], la implementación más importante existente en términos de usabilidad, aceptación y soporte, capaz de ejecutar todas las operaciones que puede soportar una versión del SOS (muchas otras versiones solo implementan las operaciones básicas obligatorias). El SOS en SAFE-ECH utiliza la base de datos PostGreSQL con soporte PosGis para los metadatos geoespaciales.

- **Un procesador de eventos complejos (CEP)**, que procesa los eventos que se detectan registrados y a través del SOS. El CEP tiene varias reglas que permiten detectar patrones específicos de eventos provenientes de múltiples fuentes, y definir las acciones que se desencadenan en respuesta. En las reglas del CEP se pueden utilizar tablas auxiliares, como horarios para realizar acciones específicas. El conjunto de reglas se adapta a las necesidades específicas de cada residencia. En este sentido, un administrador del sistema puede añadir, cambiar o eliminar reglas CEP, así como crear o modificar tablas auxiliares, a través de la HMI del sistema. Las reglas pueden ser definidas soportando análisis de combinaciones de eventos de gran complejidad. El motor CEP utilizado es ESPER [167], un procesador de flujos de eventos [166].

- **Un gestor de alarmas** que gestiona las alarmas y ciertas incidencias de alta prioridad detectadas por el procesador de eventos complejos. Las alarmas se gestionan de manera separada respecto a otros eventos debido a su alta prioridad. El Gestor de Alarmas utilizado es el Servicio de Alertas del Sensor (SAS) [168] dentro de la especificación SWE [144]. El SAS lanza las alertas a través de XMPP y opcionalmente a través de otros protocolos de transporte. Funciona en base al modelo publicación-suscripción: los productores de datos pueden incluir y configurar eventos de alarma, y los consumidores pueden suscribirse a ellos para recibir una notificación cada vez que el evento ocurra. La comunidad de 52º North ofrece una implementación mejorada del SAS [169], denominada Servicio de Eventos de Sensores (SES), que añade nuevas funcionalidades (por ejemplo, capacidades de filtrado avanzadas).

Soporta la identificación de diferentes tipos de eventos, que pueden ser la generación de una observación, un mensaje de estado de un sensor (por ejemplo, el estado de la batería), o un patrón más complejo. El sistema SAFE-ECH incorpora el mencionado SES 52º North [169].

- **Gestor de mensajería.** Es un intermediario que permite la comunicación entre los diferentes elementos del sistema central. También es la interfaz entre el sistema central y las fuentes de información externas. Se ha utilizado el bróker de código abierto RabbitMQ, que se basa en el protocolo AMQP para mensajería [40].

4.6.4. Nivel de Aquisición y Actuación

El esquema de módulos utilizados en los procesos de adquisición de datos de sensores y actuaciones en una residencia por el sistema SAFE-ECH se puede ver en la

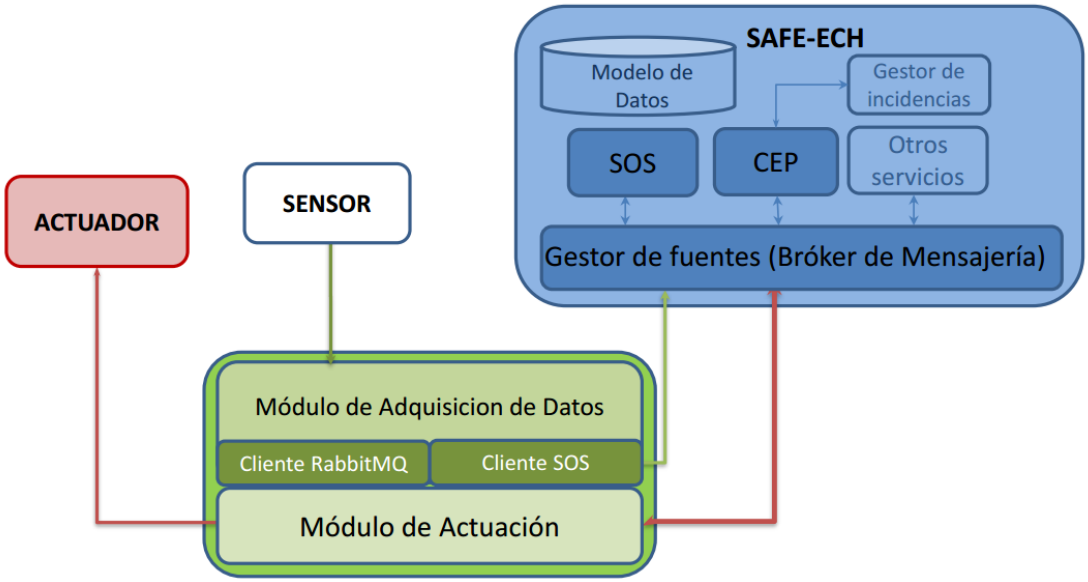


Figura 0.4. Esto incluye las redes de sensores integradas en la residencia, la red de actuadores y los módulos de adquisición de datos y de actuación en un servidor central de la residencia.

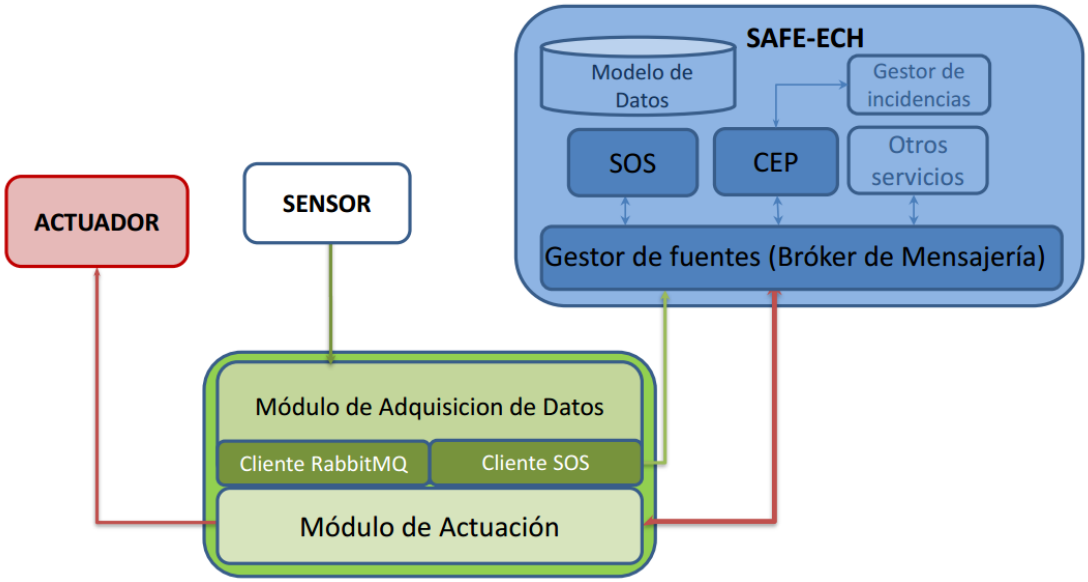


Figura 0.4 Módulos externos de actuación y adquisición de datos de SAFE-ECH

Las residencias para su monitorización y control inteligente estarán sensorizadas, con sensores instalados para detectar eventos y proporcionar información IoT de medidas, y actuadores que permitirán actuaciones automáticas en el entorno de la residencia, la aplicación de respuestas inteligentes a distintos eventos y actuaciones a distancia por parte de trabajadores desde el puesto de control. Esto permite la creación de un entorno inteligente orientado a mejorar el bienestar, la calidad de vida y la seguridad de los residentes. Los dispositivos inteligentes instalados en las residencias para soportar los casos de uso definidos, ya mencionados en un apartado anterior, son los siguientes: sensor de humo, tirador de emergencia o botón de pánico, terminal de comunicaciones, sensor de temperatura, dispositivo de control de acceso, cierre magnético de puertas, sensor de presión (variantes cama, silla y suelo), actuador de iluminación, sensores de enuresis, pulseras de localización, sensor y actuador del aire acondicionado, sensor de luz, y móviles. El sistema es flexible y admite la inclusión de nuevos sensores, medidas, respuestas, actuadores y servicios.

Los datos recogidos por los sensores se preparan por los drivers (incluidos en el dispositivo que integra el sensor o grupo de sensores) para su envío a través de su interfaz de red por la red local de comunicaciones (LAN) de la residencia. Los sensores fijos utilizan una interfaz de red cableada, mientras que los móviles utilizan una

interfaz WiFi. Estos datos de monitorización serán recogidos en el servidor local de la residencia, en el servicio de adquisición de datos. El conjunto de sensores monitorizan eventos y elementos bajo observación en la residencia que ayuden a su gestión, y a la mejora de la seguridad y comodidad de los residentes.

El servicio de adquisición de datos enviará vía HTTP la información obtenida por los sensores al sistema SAFE-ECH, mediante el uso de un cliente de mensajería (RabbitMQ [170]) y un cliente del SOS. Está información la recibirá el SOS, y se almacenará en la base de datos.

Cuando el CEP detecte que se cumple el patrón de eventos que desencadena una actuación, enviará una orden al servicio de actuación de la residencia, y desde allí será enviada al actuador.

A continuación se verá el tipo de información recogida para poder efectuar los servicios definidos en las residencias, así como las actuaciones implementadas.

Adquisición de Datos de Sensores

De manera esquemática y muy general, los distintos tipos de información de monitorización utilizada en los casos de uso y servicios implementados en el grupo de residencias, enviados al sistema central de SAFE-ECH desde el sistema de adquisición de datos se muestran en este apartado. Cada grupo engloba diferentes tipos y modelos de mensajes dentro de esa categoría.

1) Relativas a actuaciones o tareas de trabajadores
2) Relativas al servicio de aire acondicionado
3) Alarmas
4) Nivel de batería de los dispositivos
5) Control de accesos
6) Contadores
7) Control de errantes
8) Detección de Incendios
9) Alarma de intrusos
10) Iluminación

11) Localización

12) Bloqueo magnético de puertas

13) Reconocimiento y/o atención de una alarma o evento por parte de los trabajadores

14) Humedad o enuresis

Actuaciones

El centro de control de SAFE-ECH puede efectuar las siguientes actuaciones en la residencia.

1) Aire acondicionado (apagado, encendido, cambio de velocidad, temperatura o modo)

2) Accesos a la residencia (apertura o cierre de puertas)

3) Alarma de intrusos (activación de zona o sensores en concreto, desactivación, desactivación de una alarma activa)

4) Iluminación (encendido o apagado)

5) Bloqueos magnéticos de puertas (bloqueo o desbloqueo de puertas)

4.6.5. Privacidad y Seguridad

En los entornos médicos, así como en AAL, la seguridad y privacidad tienen una importancia crítica debido al uso de datos sensibles de usuarios finales (mayormente, su información de monitorización y fichas personales). Por otro lado, tanto la seguridad, la privacidad como la fiabilidad son aspectos muy importantes en IoT que se deben tener en cuenta de manera imperativa en el diseño de cualquier sistema. La heterogeneidad de los elementos de IoT, los escasos recursos de muchos objetos inteligentes y la cantidad masiva de dispositivos y datos generados representan importantes dificultades que hay que superar para poder garantizar estos aspectos.

En el sistema SAFE-ECH se ha incluido por diseño seguridad y privacidad de manera transversal a todos los niveles (Figura 4.2), con el fin de garantizarlas de manera global en este tipo de sistema AAL.

Los principales riesgos para la privacidad, la seguridad y la fiabilidad identificados para este sistema son:

- la manipulación externa de los datos y las órdenes de gestión
- la intercepción externa de la información por elementos digitales o personas no autorizadas a su acceso
- la aceptación de mensajes y datos de fuentes falsas y fraudulentas en el sistema como si procediesen de fuentes legítimas
- el acceso de usuarios no autorizados en el sistema

La seguridad global del sistema debe ser entendida en cada nivel - a nivel de comunicaciones, información, control de acceso y adquisición y actuación-, teniendo en cuenta que la información gestionada puede ser sensible o crítica, siendo en algunos casos de tipo médico o de localización de las personas, y requiere privacidad, fiabilidad e integridad.

Para evitar estos problemas de seguridad y privacidad, se han aplicado diversas medidas de seguridad en los distintos niveles de nuestro sistema (Comunicaciones, Servicio, Adquisición de Datos y Actuación) y en los distintos elementos que lo componen:

- Todas las interfaces de acceso externo al sistema central (HMI, SOS, API) cuentan con mecanismos de protección frente a inyección de código (SQL, XML o HTML), filtrado de entradas con formato erróneo o con algún otro indicativo de ser no válidas, y restricciones de acceso.
- Como elemento intermediario en el sistema, el SOS proporciona algunas medidas de seguridad para permitir sólo el acceso autorizado. La interacción externa con el SOS (desde fuera del sistema central) requiere el uso del bróker, en el que recae la responsabilidad de garantizar completamente la seguridad. Por otro lado, dentro del sistema central, el SOS es accedido por elementos internos que están a su vez protegidos de accesos externos no autorizados, además de contarse con protección de acceso general al servidor del sistema. El servicio web para acceder a la información del sistema SAFE-ECH (el cual interactúa con el SOS) puede tener restricciones de IP y protección por contraseña. Además, el SOS a su vez también tiene medidas de seguridad que pueden reforzar la seguridad general de todo el sistema. El SOS sólo acepta los datos de los sensores de las IPs autorizadas y esta acción está protegida por una contraseña (autenticación).
- El gestor de mensajería utiliza protección por contraseña, detección de IP para comprobar que la fuente utilizada es la correcta, y uso de certificados y

conexión segura. Además, su uso previene completamente la pérdida de mensajes en caso de sobrecarga.

- Los sensores y actuadores están protegidos físicamente y no son directamente accesibles, para impedir la manipulación no autorizada. Su configuración tiene como objetivo maximizar la seguridad. En todas las comunicaciones WiFi se utiliza el cifrado AES. Se han tenido en cuenta los casos habituales de fallo de batería, interferencias, error de comunicación, así como las acciones adecuadas a realizar en estos casos para garantizar la seguridad en el sistema, evitando que se puedan generar agujeros de seguridad que pudiesen ser explotados en estos casos.
- El acceso al sistema a través de la interfaz hombre-máquina (HMI), disponible desde una interfaz web, está protegido mediante autenticación de inicio de sesión con la opción de emplear también autenticación federada (mediante el uso de proveedores de identidad y de servicios). Las comunicaciones con el HMI están encriptadas con cifrado. Además, se ha tenido en cuenta la situación de error de red en las comunicaciones para prevenir posibles agujeros de seguridad aprovechando esta situación.
- La configuración del servidor web donde están alojados estos componentes impide el acceso externo a rutas y recursos del sitio web. También solo los puertos necesarios en el sistema están abiertos externamente desde dentro de una VPN, no pudiendo ser accedidos desde fuera. En este sentido, por ejemplo, operaciones del API que no se esperan utilizarse fuera del HMI no son accesibles, pudiéndose cambiar en un futuro si se decidiese explotar su funcionalidad de una manera distinta. También el API requiere autenticación previa, y utiliza variables de sesión.

Respecto a la privacidad, hay que destacar que la implementación que se ha hecho de SAFE-ECH en residencias proporciona un control no invasivo sobre los residentes debido a la elección de sensores, tipo de monitorización y servicios. La monitorización de una persona directa o indirectamente en un entorno inteligente puede cuestionarse éticamente desde un punto de vista de invasión de privacidad, y hay una gran diferencia en este sentido entre la utilización de sistemas y métodos no invasivos y, por otro lado, técnicas que invaden la privacidad. Como ejemplo comparativo se pueden mencionar por ejemplo, la gran diferencia que existe entre los detectores de caídas por detección de movimiento mediante análisis de Inteligencia Artificial sobre vídeos (que requiere cámaras monitorizando el domicilio de una persona anciana),

frente al uso de acelerómetros portables en el bolsillo. El primer método es altamente invasivo ya que recoge imágenes de la persona en todo momento dentro del entorno privado de su domicilio, mientras que el segundo, al utilizar solamente un sensor de aceleración portable en el bolsillo, permite una mayor privacidad.

En el sistema SAFE-ECH desplegado en el grupo de residencias, debido a una correcta y cuidadosa selección de casos de uso y tipo de monitorización, se garantiza y preserva un alto grado de privacidad a los residentes, a la vez que se ofrece un servicio AAL muy completo. Por otro lado, los mecanismos de seguridad del sistema garantizan también privacidad al evitar que datos sensibles pudiesen ser accedidos por terceros.

4.6.6. Capa de Semántica e Inteligencia del sistema

4.6.6.1 *Semántica del sistema*

En el sistema SAFE-ECH, la información proporcionada por los sensores está representada siguiendo un modelo de información (codificación, estructura y vocabulario) descrito en esta sección, que recoge su significado de una manera estructurada y no ambigua que constituye la semántica del sistema. El soporte semántico a la información IoT permite la interoperabilidad de la información a distintos niveles en este sistema, además de en sistemas adheridos a un estándar similar. Como información adicional, en este apartado se añade también información sobre el modelo y base de datos en que se almacena la información generada en el sistema.

Soporte semántico e interoperabilidad

El SWE proporciona una estructura y codificación adecuada para registrar sensores, actuadores y lecturas de sensores: las especificaciones SensorML [147] y Observations&Measurements (O&M) del OGC [145] [171]. Mientras SensorML permite la descripción de dispositivos inteligentes IoT, O&M describe de forma precisa sus observaciones y medidas realizadas. Una codificación XML de este modelo conceptual se define en [172], y es usada por el SOS para la gestión de la información de sensores. La información no está almacenada en RDF o OWL (que tiene la capacidad de soportar triples -anotaciones y relaciones semánticas), sino en simple XML, pero es posible una fácil adaptación a RDF [150][34].

El modelo de información básico de observación definido en O&M se puede observar en el siguiente diagrama.

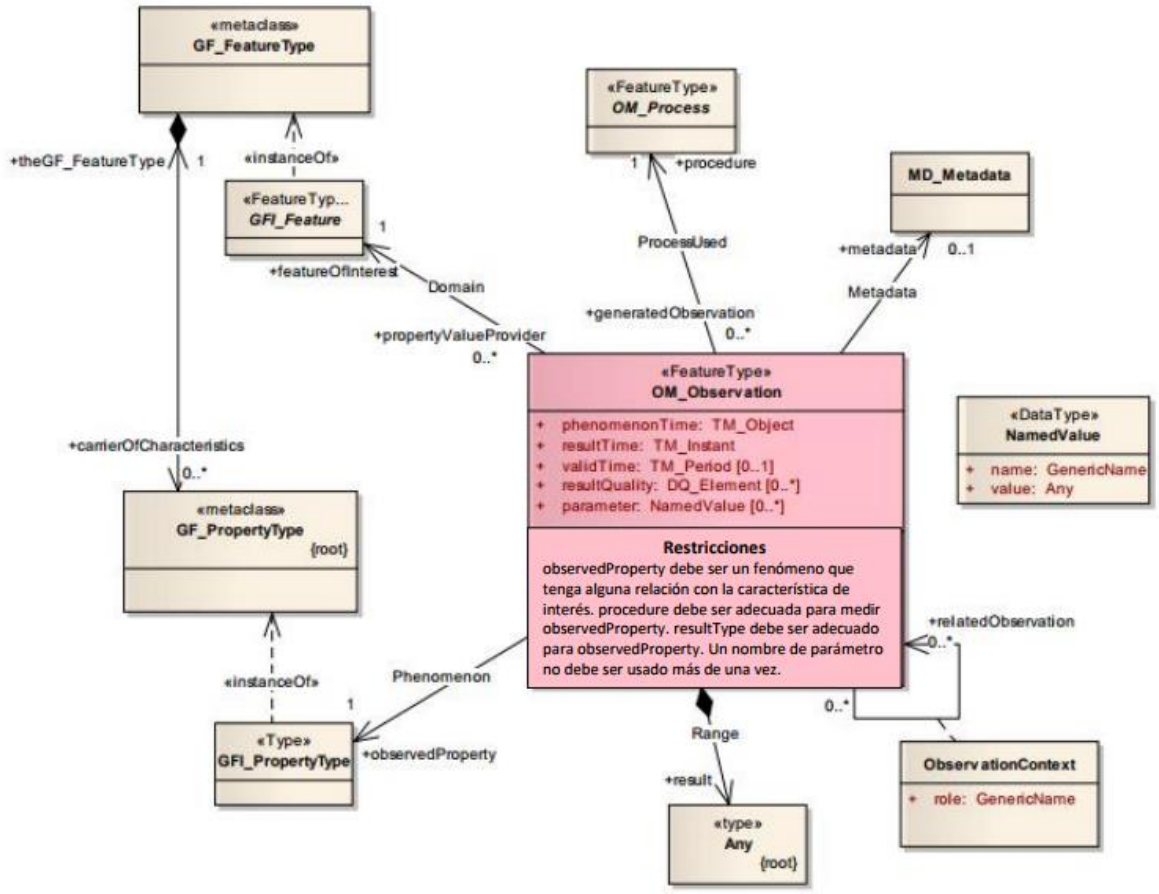


Figura 4.5– Modelo O&M básico para la descripción de una observación (imagen adaptada de la fuente: XX)

Para habilitarse la interoperabilidad semántica además de proporcionarse una estructura y codificación para los datos capaz de soportar este tipo de información conformando un modelo genérico y amplio, hace falta proporcionar un vocabulario común para los tipos de términos utilizados, de manera que su interpretación sea no ambigua y pueda ser automática. Las especificaciones del SOS y el SWE permiten que el modelo de datos utilizado sea determinado por el sistema local de sensores integrado (no así la estructura y codificación de la información). En nuestro caso, aunque podría haber sido utilizada una ontología capaz de cubrir los términos

necesarios (e.g. W3C SSN [71] o ETSI SAREF [78], especialmente diseñadas para soportar información IoT), optamos por crear un vocabulario común para todas las instancias de SAFE-ECH que cubre los siguientes conceptos O&M: procedures, offerings, observedProperty, featureOfInterest. Está publicado en la web del proyecto SAFE-ECH [161] y es ampliable en el caso de necesitarse algún término nuevo.

El SOS en sí no permite la interoperabilidad semántica, aunque proporciona elementos importantes para conseguirla, ya que además de una estructura común y codificación para los datos de los sensores se debe proporcionar un vocabulario común para los términos utilizados en los registros de las medidas (como tipo de sensor, tipo de magnitud medida, etc..) [150]. Pero en el sistema SAFE-ECH, que integra un SOS, sí se ha definido este vocabulario. Al tratarse de un modelo de información común que permite la correcta interpretación de la información de forma inambigua por los distintos sistemas que implementen este estándar, permite la habilitación de interoperabilidad semántica. Hay que notar, que en el caso de decidirse interesante en un futuro utilizarse en su lugar conceptos ya definidos en la ontología, el cambio sería relativamente sencillo (actualización de la página de referencia del vocabulario y cambios sencillos en el software).

Por otro lado, a un nivel inferior, tener definida una sintaxis o formato de datos común (en XML [173] o JSON [174]) que usar a la hora de gestionar la información desde la interfaz del SOS habilita a su vez la interoperabilidad sintáctica.

Los sistemas entre los cuales se puede habilitar directamente interoperabilidad semántica serían:

- Los sistemas de residencias integrados en una instancia global de SAFE-ECH, lo que permite la gestión múltiple. Hay que notar que generalmente un grupo de residencias gestionado no tiene necesariamente el mismo modelo de información en todas las residencias, y tampoco es normalmente un modelo unificado y genérico, sino bastante heterogéneo, según los datos empíricos observados por los socios expertos en gestión de residencias y en la tendencia general entre sistemas IoT [175] [34][73].
- Las residencias que utilizan el sistema SAFE-ECH en general, aunque no estén asociadas a una misma instancia de gestión. Al utilizar estándares y un vocabulario común su información es interoperable, y podría ser utilizada/entendida entre ellos si decidieran hacerlo.

- Sistemas u otras entidades (como aplicaciones) que utilicen los estándares del SOS y puedan aplicar el vocabulario diseñado. Esto es especialmente interesante en el caso de aplicaciones diseñadas para sistemas SOS que puedan extender la funcionalidad del sistema. Podrían ser utilizadas por todas las entidades de SAFE-ECH, y también tendrían la posibilidad de poder interoperar datos con otros sistemas o aplicaciones basadas en los estándares SWE si se viese valor en ello y fuese útil para su finalidad.

Aparte, otras ventajas de la habilitación de la interoperabilidad semántica es que en el caso de análisis inteligente de los datos con métodos de Inteligencia Artificial el uso de una codificación, estructura y vocabulario común permite evitar el coste de un preprocesado de los datos, pérdida de información, y consigue un mayor enriquecimiento de los datos, permitiendo análisis más fructíferos y de mayor valor.

En el modelo de datos se han añadido tablas auxiliares que no representan un obstáculo para el uso de este modelo o la información almacenada por otros sistemas externos que usen los estándares del SOS y el SWE: simplemente añaden un soporte para datos de gestión de residencia que son transparentes para sistemas que solo se centren en el uso de datos de sensores.

Modelo de datos

El modelo de datos representa la forma de referenciar todos los elementos necesarios en el sistema, su forma de ser almacenados y su relación con otros elementos.

El modelo de datos utilizado en SAFE-ECH está basado principalmente en el modelo de datos del SOS. El uso de este modelo es clave para la gestión de la información IoT de sensores y actuadores. Se ha extendido este modelo agregando tablas adicionales para la gestión de la residencia y para el procesamiento de eventos complejos realizado por el CEP.

Como base de datos se ha escogido PostGRESL [176], con soporte POSTGIS [177] de geoposición, el cual permite la georreferenciación de cualquier elemento almacenado, así como la aplicación de operaciones geoespaciales. Tanto el HMI, el CEP y el SOS, elementos de la arquitectura SAFE-ECH, tienen acceso a la base de datos.

Modelo de datos del SOS

El Servicio de Observación de Sensores (SOS) utiliza su modelo de datos propios para el registro de observaciones y medidas de sensores. Este modelo es complejo y busca

dar un soporte apropiado y muy completo para el tipo de información generada por objetos inteligentes IoT, y sus datos y metadatos asociados. Este modelo de datos permite la gestión de datos y metadatos de sensores, actuadores y redes de objetos inteligentes, soportando la definición de topologías, operaciones espaciales, agregados de sensores, y uso avanzado de información geoespacial. Puede ser consultado en [152].

En este modelo de datos, de gran complejidad, los conceptos más importantes son:

- Procedure – Sensores o actuadores
- observedProperty – Magnitud observada o medida (ej. temperatura)
- featureOfInterest – Característica relevante a tener en cuenta en la evaluación de la medida que no corresponde a la magnitud medida. Por ejemplo, la posición del sensor.
- Observation: medida u observación realizada por un sensor
- Result: resultado de la medida
- PhenomenonTime: tiempo en que se realizó la medida
- resultTime: tiempo en que se generó el mensaje con la medida

Tablas auxiliares de gestión de la residencia

Se ha considerado necesario realizar una pequeña extensión al modelo de datos inicial de SOS incluyendo tablas auxiliares con información de gestión de la residencia, en lugar de utilizarse otra base de datos externa a la empleada para recoger los datos de sensores. El modelo de datos del SOS ofrece un gran soporte para la gestión de la información IoT de objetos inteligentes, pero no comprende otro tipo de información relevante para la gestión de la residencia. Por ello se han agregado una serie de tablas auxiliares:

- Trabajadores (nombre, rol e id)
- Residentes
- Habitaciones & Plaza A/B
- Medicación residentes
- Errantes
- Acompañantes autorizados (asociados a residentes)
- Gestión de pañales
- Horarios de activación de alarmas (una tabla por tipo)

- Permisos de acceso de trabajadores y tiempo de validez

En el caso de ser necesario, el gestor de sistemas podría añadir otras tablas auxiliares. Estas tablas pueden ser accedidas y modificadas desde el servicio web de configuración del sistema en el HMI.

Tablas auxiliares para el modelo de datos del CEP

También es necesaria una tabla para las reglas de CEP, que permite el análisis de eventos complejos y la respuesta inteligente asociada del sistema. Esta tabla se relaciona con otras tablas del modelo de dato del SOS, sensores y las tablas auxiliares de gestión.

Para la generación de la condición de activación del CEP, se pueden poner múltiples condiciones concatenadas con Y u O lógicos. Estas condiciones se refieren al valor de un sensor concreto o conjunto de sensores de un tipo (NOT, >,<,=, o conjunto de posibles estados), o bien a una franja horaria. Las respuestas pueden ser la generación de eventos o alarmas, o una actuación (como por ejemplo la desactivación de una alarma).

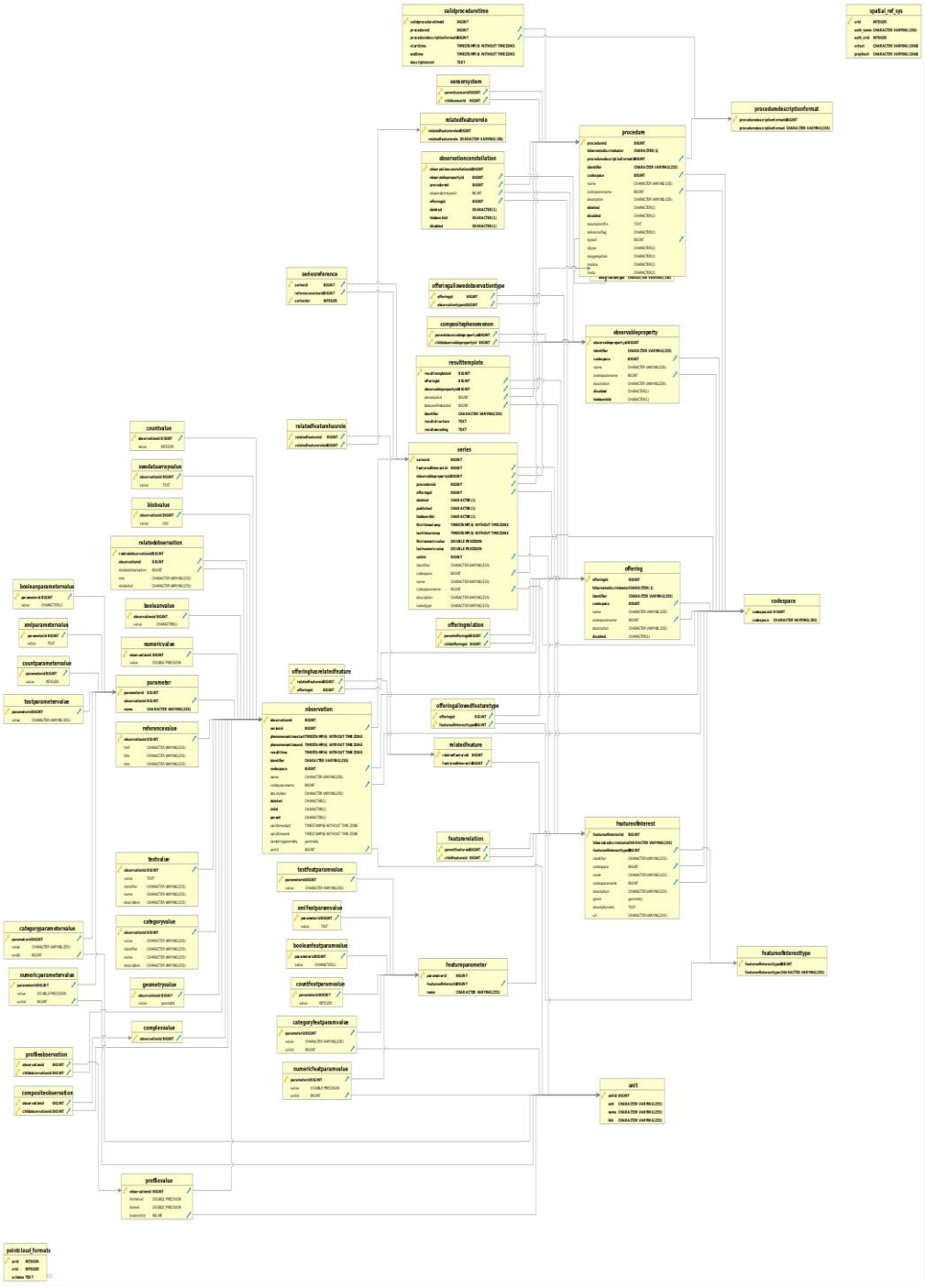


Figura 4.6 Modelo simplificado de datos de una versión anterior de SOS. El modelo de datos actual del SOS 2.0 es una extensión del mismo y su representación no es visualizable en formato A4.

4.6.6.2 *Inteligencia del sistema: reglas de razonamiento lógico*

Un elemento clave para dotar al sistema de auto-gestión e inteligencia es el servicio CEP (Complex Event Processor) que permite el procesamiento de datos de múltiples fuentes para inferir eventos o patrones que implican una combinación de circunstancias o eventos compleja. El servicio CEP es el responsable de analizar los eventos y datos del sistema, y efectuar acciones determinadas al cumplirse ciertos patrones complejos. Este procesado lógico de la información de monitorización proporcionada mayormente por sensores IoT (IoT big data) constituye la inteligencia del sistema. Las reglas lógicas establecidas para los distintos casos de uso pueden verse seguidamente en este apartado (Tabla 4.1) y son codificadas y almacenadas internamente como líneas de programación en lenguaje Java, al utilizarse el motor ESPER. Estas reglas pueden ser modificadas o eliminadas desde el HMI, que permite su configuración. Así mismo, pueden ser añadidas nuevas reglas añadiendo condiciones a cumplir y respuestas. Los elementos para generar reglas son los usuarios, habitaciones, sensores, actuadores, alarmas, eventos (determinada información de monitorización), temporizadores e inclusive tablas de usuarios (por ejemplo de acompañantes autorizados). La generación de reglas desde el entorno gráfico es sencilla y no requiere de conocimientos informáticos sino de sentido lógico. Para una mejor gestión y seguridad, solo disponen generalmente de permisos para crearlas los usuarios gestores y no en cambio la mayoría de trabajadores. El uso de un Procesador de Eventos Complejos aporta una significante mejoría a los típicos sistemas de gestión de residencias propietarios que no suelen poder hacer análisis tan profundo o complejo de una combinación de eventos, ni programar análisis de forma sistemática y permitir a usuarios no programadores generarlos fácilmente.

Tabla 4.1 – Reglas programas de análisis de eventos y repuestas

CONTROL DE ERRANTES
• Errante detectado por RFID + Franja horaria de salida permitida + (puerta cerrada) -> Apertura de puerta + Registro de salidas (errante) • Errante detectado por RFID + Franja horaria de salida NO permitida + puerta cerrada (ausencia de -> Registro de intento de salida o acercamiento al acceso (errante)

• Errante detectado por RFID + Franja horaria de salida NO permitida + puerta abierta -> Apertura de puerta + Registro de salidas (errante) • Errante detectado por RFID + Franja horaria de salida permitida -> Apertura de puerta + Registro de salidas (errante) • Errante detectado por RFID + Franja horaria de salida permitida con acompañante + Acompañante + -> Apertura de puerta + Registro de salidas (errante+acompañante) • Errante detectado por RFID + Franja horaria de salida NO permitida con o sin acompañante + Acompañante + -> Registro de intento de salida o acercamiento al acceso (errante+acompañante)
ALARMAS MÉDICAS
• Alarma médica (tirador o pulsador) + ausencia de atención de alarma + ausencia de repetición -> Alarma en el sistema + Registro de alarma • Alarma médica (tirador o pulsador) + repetición de la alarma + ausencia de atención de alarma -> Alarma URGENTE • (Alarmas en las que haya que poner relanzamiento) – ausencia de atención en x minutos -> Relanzamiento de la alarma • Alarma médica + atención de alarma –> Cambio estado en registro de alarma (en atención) + desactivación sonido o visión en primer plano de alarma • Alarma médica+ finalización de alarma -> Cambio estado en registro de alarma (finalizada)
ELIMINACIÓN DE SUJECIONES – ALARMA DE PRESIÓN EN SILLA O CAMA
• (Inmediata) Detección de levantamiento –> Alarma • (Tiempo de espera de regreso) Detección de levantamiento + tiempo de espera no vencido + detección de regreso -> Nada • (Tiempo de espera de regreso) Detección de levantamiento + tiempo de espera vencido + ausencia detección de regreso -> Alarma
ACCIÓN DE TRABAJADORES
Actuación para borrar la acción anterior registrada por el cuidador en la habitación, por un error al marcarla + diferencia de tiempo pequeña (<5min)-> Borrarla o indicar en algún campo que no es válida

AIRE ACONDICIONADO
Existe una programación automática de la configuración de las unidades de aire, lo que permite encender, apagar, cambiar la temperatura dependiendo de la franja horaria.
ILUMINACIÓN
Tabla de iluminación – zonas de iluminación (una o varias), horas de encendido y apagado.

4.6.7. Interfaces del sistema

4.6.7.1 *HMI (Interfaz Hombre-Máquina)*

El HMI ha sido desarrollado utilizando los lenguajes Java, HTML, Javascript además del uso de Maven para integrar distintas librerías y módulos. El HMI o Interfaz Hombre-Máquina es una interfaz web online que permite acceso bajo autenticación a los distintos tipos de usuarios autorizados (gestores y cuidadores) dentro del ámbito del servicio a la residencia. Soporta el uso de cifrado y conexión segura. Es una interfaz gráfica para la gestión (GUI) en la que se ha priorizado la usabilidad, claridad y sencillez y no requiere conocimientos informáticos.

Dispone de acceso ubicuo mediante conexión al servidor a través de Internet, y puede ser accedido por cualquier trabajador que disponga de una tableta o un móvil, o desde el ordenador del puesto de control. Permite ver las alarmas y los eventos en tiempo real, dando la posibilidad del acceso a los datos históricos de determinados sensores, alarmas, habitaciones o usuarios. Además, aporta una visión global de la situación de la residencia al permitir ver los sensores y alarmas en un mapa, y un listado de eventos y alarmas recientes, en tiempo real.

Consta de:

- Pantalla de autenticación de usuario o log-in
- Un panel principal, donde se puede ver en tiempo real los eventos, alarmas y la situación global de la residencia gráficamente
- Acceso a datos históricos (información de sensores, eventos y alarmas)
- Acceso a la configuración del sistema (reglas CEP y tablas de gestión)

- Acceso al modo multirresidencia en grupos de residencias bajo gestión jerárquica en el sistema

Su objetivo es proporcionar a todos los trabajadores información útil sobre el funcionamiento de la residencia, estar informado de los eventos en tiempo real y recibir alarmas. Además de poder acceder a información de históricos, a la configuración del sistema o a funciones de gestión multirresidencia si se tienen los permisos necesarios.

Panel Principal

El panel principal tiene la función de aportar información clave de la situación de la residencia al gestor o trabajador en tiempo real y consta de los siguientes elementos:

- -un mapa de la residencia donde está indicado el tipo y la posición de todos los sensores y elementos geolocalizados, así como las alertas generadas en ellos. Al pasar el ratón sobre una alerta o un sensor se despliega información asociada. Las alertas pueden verse también en el panel de alarmas
- -un panel de alarmas recientes, donde pueden verse todas las alarmas activas
- -un panel de eventos, donde se visualiza en tiempo real los distintos eventos que se van monitorizando en la residencia.
- -acceso a la pantalla de gestión de históricos
- -acceso a la pantalla de configuración del sistema

Históricos

El HMI permite el acceso a los históricos de los distintos elementos (usuarios, sensores, habitaciones o tipos de evento o alarma) en el periodo de tiempo que se seleccione.

Para un rango temporal, se puede seleccionar un sensor en concreto por ID, un tipo de sensor en una habitación concreta, o todas las medidas o eventos de un tipo de sensor (p.e. sensor de alarma médica, detección intrusos, etc..). Lo mismo sucede para eventos y alarmas. Las alarmas, eventos y mediciones relacionados con un usuario pueden obtenerse usando como identificador del usuario su número de habitación y plaza (A o B), y en este caso es posible también determinar el tipo de alarma o de evento (alarma médica, acceso habitación, etc..) u obtener todos los relacionados con el usuario en el rango de tiempo determinado.

Configuración

Los cambios en la configuración del sistema son pueden realizarlos usuarios con permisos de gestor. Permite el cambio de reglas de control, la gestión de la red de sensores y actuadores (incluir o eliminar sensores) y la actualización de las tablas auxiliares de control de la residencia.

Gestión Multirresidencia

Desde el HMI se puede acceder al modo de gestión multiresidencia, y obtener información de otras residencias si se dispone permiso de gestión sobre ellas. Será posible acceder al panel principal, configuración e históricos de otras residencias integradas.

Las residencias integradas en esta primera instancia de SAFE-ECH son las siete residencias del Grupo SOLIMAR en la Comunidad Valenciana, y están integradas geoespacialmente en el sistema de mapas OpenStreetMap. Se puede navegar en el mapa proporcionado por este sistema en la interfaz multirresidencia, y los mapas de la residencia pueden verse como una capa superpuesta integrada en las coordenadas correspondientes a su posición real. En la duración del proyecto se integró de manera completa la residencia piloto, y se planeó la futura integración de las otras seis residencias (las cuales estaban conectadas sin usarse datos reales, solo simulación).

La integración de nuevas residencias en el sistema es sencilla aportando el mapa de la residencia, su geoposición, los identificadores y el tipo de los sensores y su geoposición inicial, además de los casos de uso integrados (si se añade uno aún no registrado). Por seguridad, esta operación solo puede hacerla el gestor del sistema de sistemas. También la operación de modificación o eliminación de una residencia es en esta misma línea sencilla y solo puede realizarse por el gestor.

La gestión multirresidencia no solo permite acceder a datos de sensores, eventos y alarmas de otras residencias y crea un HMI múltiple. También desde la interfaz global se pueden acceder a un panel de alarmas globales de todas las residencias, y datos estadísticos globales. Su mayor utilidad reside en el análisis potencial de datos globales, permitiendo ver detalles que puedan llevar a una mayor optimización del servicio en residencias concretas. También permite la monitorización de varias residencias desde un solo puesto de control en situaciones que así lo requieran.

4.6.7.2 *API*

El API del sistema central tiene una serie de operaciones para la gestión de la residencia, accesibles indirectamente desde el HMI (modo gestión monorresidencia o multirresidencia) siempre que se haya generado la variable de sesión de autenticación de usuario autorizado y se acceda bajo TLS y cifrado. Constituye un API REST.

Tabla 4.2 – Funciones cubiertas por las distintas operaciones del API

Interacciones con tablas de configuración
• Habilitador de eventos de aviso a entrada a zonas (localización) • Inhibición de alarmas en determinada franja horaria • Bloqueo y desbloqueo contactos magnéticos de puertas de emergencia en determinada franja horaria. • Códigos de actuaciones de trabajadores • Programación de la iluminación • Programación del aire acondicionado • Habilitación/deshabilitación de alarmas de tirador de emergencia • Tabla de control de accesos: identidad, identificador y permisos • Habilitador de alarma de errantes, y habilitador de acompañantes que evitan el lanzamiento de la alarma. • Valores límite y umbrales de alarmas
Envío de órdenes de actuación:
• Apagado/encendido de luces • Apagado/encendido/regulación de temperatura del aire acondicionado • Consulta de estado de determinados sensores asociados a actuadores (temperatura, temperatura objetivo, estado encendido o apagado de las luces)
Consulta de información de monitorización almacenada en la BBDD del SOS
• Consulta de información de sensores y alarmas en tiempo real • Consulta de históricos de información de sensores y alarmas
Configuración de la red de sensores:
• Insertar sensores • Quitar sensores • Habilitar/deshabilitar sensores

Monitorización de Alarmas:
• Habilitar/deshabilitar alarmas • Consulta histórico de alarmas • Desactivar alarmas

Las opciones que proporciona el API son accesibles desde el HMI, que proporciona una interfaz gráfica para el acceso a sus operaciones (configuración e históricos). Tiene incorporados mecanismos de seguridad tales como requerir autenticación de usuario, y protección contra inyección de código o filtrado de entradas y parámetros que se detecten como erróneos o incompatibles.

4.6.7.3 *Interfaz de comunicación con el SOS*

El SOS proporciona una interfaz de comunicación para el envío y acceso a la información de las redes de sensores y actuadores de la residencia. En línea con el concepto de Sensor Web (SWE) permite el acceso o el envío de esta información de una red de sensores mediante el uso de los mismos protocolos (HTTP o HTTPS) y APIs (REST API) para el acceso a una web.

El SOS permite una serie de operaciones accesibles según los perfiles implementados: perfil básico, perfil transaccional, perfil mejorado y perfil completo. El soporte del perfil básico es obligatorio para cualquier implementación SOS, mientras que el resto de perfiles son opcionales. Nuestra implementación (52º North SOS 2.0) permite el uso de todas las operaciones (perfil completo).

Estas operaciones están codificadas usando los estándares O&M o SensorML del SWE y el formato XML, aunque opcionalmente se permite utilizar el formato JSON en algunas de ellas. Se prevé que en futuras implementaciones del SOS todas ellas soportaran el uso de la estructura de datos JSON, más ligera y eficiente, que permite velocidades mayores de trabajo y exige menor carga computacional [159][160].

El acceso al SOS está protegido. Externamente la recepción de los datos de los sensores enviados por el gestor de mensajería está protegida con el uso de contraseña y restricción de IP de origen en el gestor, además de uso de cifrado y TLS. Respecto al resto de operaciones distintas de la inserción de sensores u observaciones, solo el sistema central puede acceder a ellas a través de la interfaz del SOS, no siendo posible su acceso externo.

Tabla 4.3 – Operaciones de la interfaz del SOS según el tipo de perfil

Perfil básico
-GetCapabilities: Identificación de sensores disponibles con cierta capacidad de filtrado de parámetros - GetObservation: Acceso a los datos de sensores - DescribeSensor: Acceso a la descripción de los sensores
Perfil transaccional
- RegisterSensor: Registro de un sensor nuevo - InsertObservation: Inserción de una nueva medida
Perfil mejorado
-GetResult: Operación eficiente para solicitar repetidamente datos de sensores - GetFeatureOfInterest: Devuelve la descripción de una característica o dato de interés asociado a una medida diferente de la magnitud medida o el tiempo, como podría ser por ejemplo la localidad o el nombre de la residencia. - GetFeatureOfInterestTime: El tiempo para el cual se dispone de medidas para una característica de interés - DescribeFeatureOfInterest: Solicitar el esquema XML que define el formato de las características de interés - DescribeObservationType: Solicitar el esquema XML que define el formato de las observaciones - DescribeResultModel: Solicitar el esquema XML que define el formato de las medidas
Perfil completo
Todas las operaciones

4.6.8. Otras características clave del sistema

4.6.8.1 *Escalabilidad y Flexibilidad*

SAFE-ECH es escalable verticalmente (en el sentido de permitir la gestión de múltiples residencias) y horizontalmente, en el sentido de que el diseño de nuestro sistema tiene una buena escalabilidad y adaptabilidad en la integración de redes muy diferentes y heterogéneas de sensores y actuadores. Es fácil incluir nuevos elementos o modificar esas colecciones. Además, esta extensibilidad también está referida a servicios, ya los patrones de decisión de la inteligencia del sistema son configurables, y es fácil añadir, retirar o modificar servicios. De esta manera puede configurarse fácilmente para establecer entornos de Inteligencia Ambiental muy diversos (una amplia gama) en el contexto de AAL y AHA. Puede adaptarse a las necesidades específicas de cada residencia de ancianos. Además, esta flexibilidad permite una posible adaptación al ámbito de las casas inteligentes para personas mayores, y no se limita únicamente a las residencias de ancianos.

El uso de estándares abiertos permite una buena interoperabilidad, y facilita la flexibilidad y escalabilidad del sistema. En particular, la interfaz proporcionada por el SOS permite una fácil integración de los sensores.

4.6.8.2 *Geolocalización*

Este sistema permite la geolocalización de los distintos eventos, información y posición de sensores dentro de la residencia, y la integración de un mapa geolocalizado de ella. Todos los sensores están geolocalizados siguiendo los estándares de posicionamiento geospacial del OGC. La geolocalización es un aspecto importante en la información IoT que en muchas ocasiones en los sistemas clásicos es ignorada o solo parcialmente aprovechado. La implementación de información geoespacial es una valiosa herramienta que permite una visualización rápida en un mapa de la situación de la residencia, sus eventos y alarmas a los gestores y trabajadores.

También se ha creado una aplicación móvil con un sistema muy innovador de localización *indoor* basado en indicadores de localización por potencia y uso de puntos de acceso en redes WiFi [178] (el sistema de posicionamiento GPS no funciona dentro de edificios) [179][180]. Este sistema de detección de posición se utilizó en pruebas en el piloto para la localización de personas con un teléfono móvil en el cual estaba la

aplicación instalada. Su finalidad era poder explotarse para detectar con facilidad la localización de cuidadores y residentes en todo momento con fines de mejora del servicio, eficiencia y de la seguridad de los internos. Este trabajo estaba fuera de los casos de uso a cubrir y representaba un extra añadido voluntariamente al proyecto. Se hizo un estudio de su aplicación y efectividad, pero no se llegó a hacer una implementación completa en la residencia por razones fuera del ámbito técnico. El uso de datos tan sensibles como la posición de una persona en todo momento implica una profunda deliberación sobre políticas a desarrollar y acordar de mutuo acuerdo entre gestores, trabajadores, residentes y familiares, en términos éticos y legales para garantizar una máxima gestión de la privacidad y no hacer en ningún momento acciones que pudiesen considerarse invasivas. En un trabajo futuro se pretende integrar en el sistema con una gestión con altos niveles de privacidad en entornos de residencias o en ámbitos diferentes.

4.7. Validación del Sistema

Validación del sistema en residencia piloto

El sistema SAFE-ECH fue desplegado en una residencia de ancianos del grupo Georresidenciales SOLIMAR en la localidad de Sollana en España. Las principales características del piloto son las siguientes: cuenta con 136 residentes, 42 cuidadores que trabajan en tres turnos diarios y 80 habitaciones (68 dormitorios para personas mayores y 12 habitaciones comunes). Sus 136 plazas están distribuidas en 68 habitaciones, todas ellas exteriores en una superficie construida de 4.000m2, y disponiendo de más de 7.500 m2 de zona ajardinada. Los servicios que implementados en el sistema y en la residencia son la detección de intrusos, la alarma de incendios, las emergencias médicas, el control de accesos, la climatización y el servicio de iluminación inteligente. La elección de esta residencia como piloto se ha debido a sus particularidades estructurales y de ubicación, que la hacen especialmente indicada para probar determinados sistemas y servicios. Presenta una planta en dos alturas y gran extensión de zona ajardinada, con salidas el exterior que presentan cierta inseguridad para los residentes, constituyendo un escenario perfecto para probar sistemas como el control de accesos.

Para la supervisión de la residencia, se han utilizado 1378 sensores (botones de alarma de habitaciones, terminales, puntos de control de acceso, sensores de aire

acondicionado, detectores de humo). Toda la zona de la residencia dispone de conectividad a Internet para sensores y actuadores utilizando una red privada a la que solo tienen acceso los gestores de la residencia. Así, los sensores se comunican con el sistema central mediante conectividad LAN por cable, en el caso de los sensores fijos, y WiFi, en el caso de los sensores móviles. Su implementación y distribución está detallada en la próxima sección.

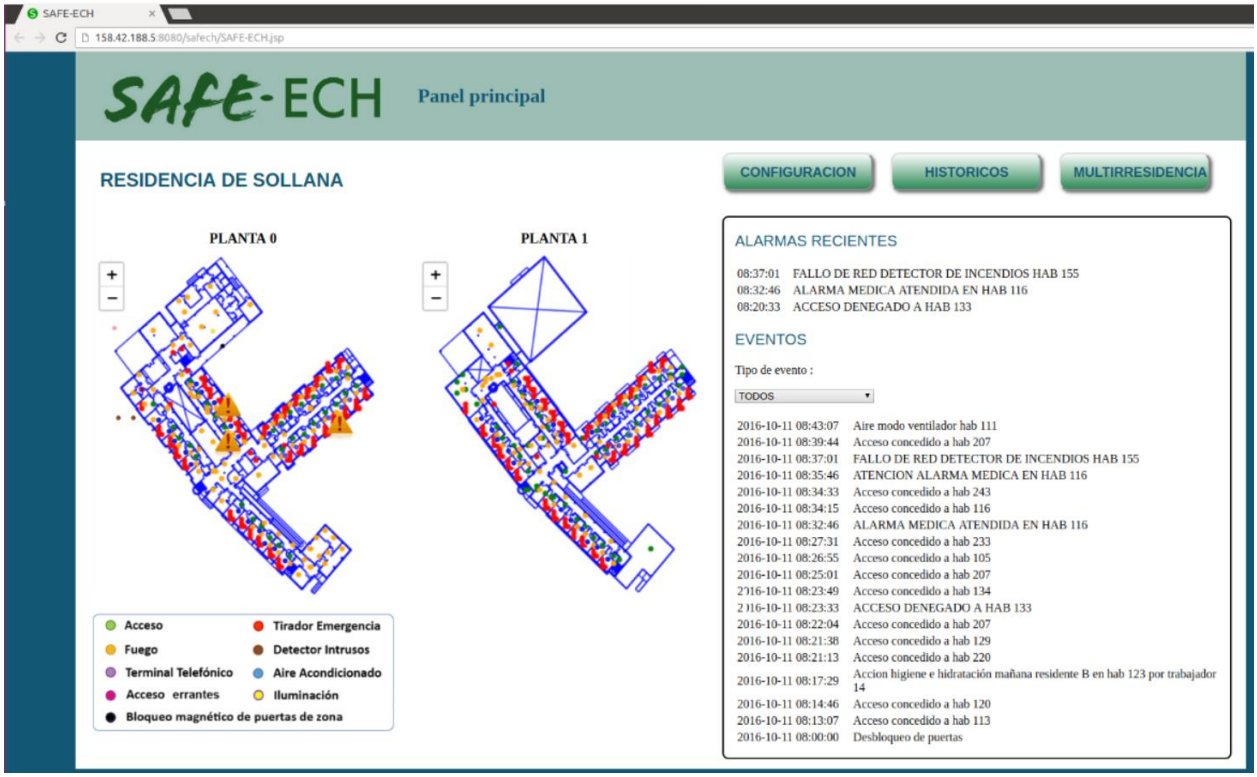


Figura4.7 Panel de control principal del HMI

El sistema SAFE-ECH recibe los datos producidos por los sensores, el componente SOS los almacena y, finalmente, el sistema los analiza. Como resultado del análisis realizado por la inteligencia del sistema, pueden producirse determinadas acciones de control: envío de notificaciones a los cuidadores, lanzamiento de alarmas si se cumplen sus condiciones de activación y envío de órdenes a actuadores. Este tipo de acciones también pueden realizarse como resultado de una programación y configuración previa del sistema sin que sean causa y efecto de eventos de

monitorización detectados por los sensores. Un ejemplo de ello, entre otros muchos, sería la activación automática de la alarma de intrusión a una hora determinada de la noche.

Los cuidadores pueden interactuar con el sistema a través de la HMI. Esta accesible de forma ubicua a los trabajadores a través de dispositivos como móviles, tabletas u ordenadores con conectividad a internet. Como consecuencia del conocimiento de la información de seguimiento relevante, los cuidadores aprecian que pueden ser más eficaces, rápidos, eficientes y tener una mejor coordinación en el servicio que prestan a las personas mayores.

Los principales servicios ofrecidos en la residencia piloto a través de SAFE-ECH son la detección de intrusos, la alarma de incendios, las emergencias médicas, el control de accesos, la regulación del aire acondicionado y el sistema de iluminación inteligente.

Estos servicios se describen con más detalle en los párrafos siguientes, y es posible observar su relación con el mapa de sensores desplegados en la residencia (Figura 4.9):

La detección de intrusos es un servicio que protege ciertos puntos de acceso de la residencia a horas específicas contra el acceso no autorizado, lanza alarmas si hay algún intento de allanamiento y mantiene las puertas cerradas a distancia. Se programa para que esté activo a unas horas determinadas (por ejemplo, por la noche) desde el sistema central.

El servicio de alarma de incendios detecta si una concentración de CO2 o CO es superior a la habitual y lanza una alarma de incendio, lo que permite un rápido desalojo y/o otras medidas de sofocación del fuego. Tener una respuesta rápida es crítico en situaciones de incendio. Los sensores de humo están distribuidos por toda la zona de la residencia, incluyendo todas las habitaciones, e informan al sistema central de la existencia de un posible incendio en su ubicación específica, y se lanza automáticamente una alarma. Esta alarma puede desactivarse manualmente, a través de la HMI del sistema central, o tras un periodo de tiempo de espera si los sensores de humo no la activan.

Emergencia médica es un servicio que pretende dar a los residentes y cuidadores una forma rápida de activar una alarma en caso de emergencia, para alertar inmediatamente al sistema y a los demás cuidadores con el fin de lograr una reacción lo más rápida y eficaz posible. Está especialmente pensado para las emergencias

sanitarias y accidentes. Para ello, muchas habitaciones de la residencia están provistas de botones o pulsadores de emergencia que pueden ser fácilmente pulsados y activados por los residentes o cuidadores en caso de emergencia. El sistema lanzará una alarma, que estará activa hasta que un cuidador informe de que la emergencia está siendo atendida. La alarma quedará entonces en estado de espera hasta que, finalmente, un cuidador la cierre cuando se resuelva. Si fuera necesario, se llamará a los servicios sanitarios. En realidad, cada una de las salas comunes (es decir, el gimnasio, el comedor, los salones y los baños), las habitaciones y los baños privados contienen al menos un botón o manipulador de emergencia, además de un comunicador de voz. Este servicio permite una rápida respuesta de los cuidadores y los servicios sanitarios en caso de accidentes, emergencias médicas o cualquier otra situación de riesgo.

Control de acceso: este servicio restringe la entrada a diferentes zonas de la residencia sólo a las personas autorizadas, por razones de seguridad y privacidad. Las puertas que limitan determinadas zonas de la residencia cuentan con un sistema de control de acceso por tarjeta que sólo permite el acceso de personas con permisos de acceso válidos. El sistema tiene un registro de residentes y cuidadores, los accesos que pueden abrir con sus tarjetas de acceso y la fecha de finalización de esos permisos. Si el acceso está autorizado, la puerta se desbloquea y se abre. Este sistema garantiza la privacidad de los residentes en las habitaciones en las que viven, a las que sólo pueden acceder ellos, los cuidadores o el personal del servicio de limpieza. Además, este servicio evita la entrada de intrusos en otras zonas de la residencia.

Aire acondicionado: La temperatura es regulada automáticamente por el sistema para ofrecer las condiciones ambientales más adecuadas para el confort de los antiguos residentes. Es fundamental ofrecer una temperatura adecuada como medida para prevenir problemas de salud en las personas mayores. Los aparatos de aire acondicionado tienen varios sensores y actuadores conectados al sistema. Estos sensores miden la temperatura ambiental actual, la velocidad del aire y la temperatura objetivo registrada en el dispositivo, y envían esta información al sistema central. Los actuadores pueden modificar la temperatura objetivo del dispositivo y la velocidad del aire. Desde el sistema central es posible programar la temperatura objetivo de toda la residencia o particularizarla para dispositivos específicos (por ejemplo, algunas habitaciones pueden estar vacías y no necesitan estar calientes). Además, es posible programar los tiempos, la velocidad del aire y las temperaturas

para un conjunto de aparatos de aire acondicionado, o unos específicos, a través del HMI como usuario administrador.

Servicio de iluminación inteligente: este servicio permite que las luminarias de las salas comunes de la residencia sean encendidas y apagadas automáticamente por el sistema. Los administradores del sistema pueden programar la hora de inicio y finalización de la iluminación.

Despliegue de dispositivos en Sollana

Los casos de uso y servicios requieren de la sensorización inteligente previa del edificio. Hay dispositivos de acceso, detección de humos e incendios, terminal de comunicación telefónico, acceso de errantes, tiradores o botones de emergencia, detectores de intruso por intento de apertura de puerta, aire acondicionado e iluminación inteligente. Estos dispositivos son en algunos casos un conjunto de sensores y actuadores, como en el caso de detección de intrusos (en que una actuación puede habilitar el sistema o desactivar alarmas) o aire acondicionado (hay sensores de velocidad y temperatura y actuadores).

Las 68 habitaciones para residentes tienen sensores especiales para poder garantizar al máximo su seguridad y confort. Cada dormitorio consta de:

- -un terminal de comunicaciones para poder establecer comunicación con el centro de control de la residencia, o la enfermería.
- -un tirador de emergencia en el baño para poder alertar a los trabajadores en caso de caída, para asegurar una rápida actuación en caso de alerta sanitaria
- -un pulsador de emergencia en la mesilla por cada usuario (por tanto, doble)
- -un pulsador de emergencia en la entrada
- -un actuador sobre el aire acondicionado y sensor temperatura
- -un detector de incendios
- -un dispositivo de control de acceso, que permite o no el acceso (apertura de puerta) según los permisos de la tarjeta o pulsera del usuario, y lo comunica al centro de control

Figura4.8 Habitación de residentes y distribución de sensores y actuadores

Otros sensores dispuestos en la residencia se encuentran en las salas comunes y la cocina, destacando la existencia de actuadores en el sistema de iluminación y del aire acondicionado de estas áreas. Toda el área de la residencia cuenta con sensores de humo para la prevención de incendios. En los exteriores hay dispositivos de detección de intrusos y control de errantes, además de contarse con actuadores para el bloqueo magnético de la puerta de servicio de la residencia.

La distribución de sensores a lo largo de toda la residencia puede observarse con detalle los mapas disponibles desde el HMI, donde están geolocalizados y diferenciados por tipo y función.

Figura 4.9 Distribución de los 1378 sensores de la residencia de Sollana

Validación del Ministerio de Economía y Competitividad (MINECO)

La consecución de los objetivos del proyecto RETOS SAFE-ECH se evaluó positivamente por el Ministerio de Economía y Competitividad, considerándose todos

ellos alcanzados satisfactoriamente en la evaluación realizada al final del tiempo de vida del proyecto (Septiembre 2017).

Avances asociados al sistema

Gracias al trabajo conseguido con esta implantación de nuestro sistema se han conseguido una serie de ventajas frente a otros sistemas de gestión de residencias. A continuación se resumen brevemente estas ventajas.

Desde un punto de vista técnico, nuestro sistema:

- Permite una fácil configuración de eventos complejos (detección y respuesta), mecanismos personalizados de gestión ante determinados eventos, que pueden tener en cuenta datos médicos almacenados en la base de datos. Esto se consigue principalmente como consecuencia de la integración de un procesador de eventos complejos (CEP) y hace que nuestro sistema sea más versátil, pues el tipo de casuística que puede abordarse es mucho mayor, y más dirigida al uso masivo de datos.
- Permite la integración de todo tipo de sensores, permitiendo el uso de sensores de muy distinto tipo, tecnología, fabricante y topología global de la red de sensores, como consecuencia de la interoperabilidad lograda a nivel técnico sobre sensores, actuadores y pasarelas inteligentes. Esto hace que el sistema sea mucho más flexible y escalable, al eliminar restricciones de terceros. No presenta el problema "vendor lock-in" de sistemas propietarios
- Homogenización de la información almacenada y utilizada por herramientas de gestión, utilizándose estándares abiertos OGC/SWE, con el sistema de codificación O&M. Con esto, se consigue una mayor eficiencia en la gestión de los datos, pudiéndose utilizar herramientas y sistemas de almacenaje estructurado, tales como datalakes o data warehouses.
- Uso de estándares abiertos ampliamente utilizados (paradigma SWE del OGC), lo que facilita su compatibilidad futura con otros sistemas y la comprensión de la información por otros sistemas y entidades. Esta directriz de diseño permite por tanto una mayor interoperabilidad, compatibilidad externa y escalabilidad del sistema [181].
- Interoperabilidad sintáctica y semántica de la información dentro del mismo sistema, con otras residencias del mismo grupo gestionadas por el sistema, otras residencias externas gestionadas con este sistema, y otros sistemas que

siguen los mismos estándares. Esta característica permite la comprensión y uso de la información por otras entidades y sistemas. Esto facilita por ejemplo, la ampliación del sistema con otros que puedan complementarlo y usen estos estándares, o la cooperación con otros sistemas que utilicen estos estándares. También hay que destacar que la homogeneización de la información bajo una estructura sintáctica y semántica concreta facilita enormemente el análisis inteligente bajo técnicas de Machine Learning, ya que permite un mayor enriquecimiento de los datos y también ahorra tareas de preprocesado. Interoperabilidad sintáctica y semántica de la información dentro del mismo sistema, con otras residencias del mismo grupo gestionadas por el sistema, otras residencias externas gestionadas con este sistema, y otros sistemas que siguen los mismos estándares.

- Interfaz de gran usabilidad: la interfaz hombre-máquina ha sido diseñada para priorizar la usabilidad, rápido acceso a la información clave y su facilidad de uso. Puede ser utilizada por usuarios con muy bajos conocimientos informáticos. Permite una visión global de la situación de la residencia en mapas y un panel de eventos y alarmas recientes.
- Gran accesibilidad: Acceso ubicuo a la información de gestión y monitorización del sistema: el HMI es accesible para las personas autorizadas desde cualquier punto con conectividad desde teléfonos móviles, tabletas o un ordenador. En contraste, los sistemas de gestión para esta área son típicamente accesibles solo desde un puesto de control centralizado.
- Acceso de usuarios con distintos grados de permiso y protección, lo que otorga más flexibilidad y seguridad al uso del sistema, ya que permite adecuar a cada usuario el acceso necesario, pudiendo acceder al conjunto de información que necesita, evitando riesgos, por ejemplo, de cambios accidentales en la configuración de servicios esenciales.
- Sistema extensible y escalable, pudiéndose integrar nuevos sensores, nuevos tipos de sensores y actuadores, nuevos servicios y gestión de respuestas, de manera flexible a diferencia de otros sistemas de gestión (extensibilidad horizontal con gran flexibilidad).
- Gestión de múltiples residencias. Permite la extensión jerárquica del sistema (extensibilidad vertical) permitiendo una gestión centralizada, sin implicar modificaciones en el sistema y su operativa. La arquitectura y características

de los estándares empleados permite el desarrollo de una estructura jerárquica englobando la gestión de un grupo de múltiples residencias.

- Integración y uso de elementos de geolocalización: SAFE-ECH permite la gestión de datos y metadatos geoespaciales asociados a la información obtenida por los sensores, a diferencia de muchos sistemas que no soportan e ignoran la gestión de este tipo de información, que tiene una especial relevancia en el paradigma IoT. El uso de información de geolocalización permite explotar de forma mucho más completa el potencial del uso de IoT. Permite geolocalizar sensores y su información, un análisis posterior de los datos con esta información añadida (dato enriquecido), servicios como mostrar en un mapa de la residencia la posición de sensores y eventos, además de poder ofrecer otros en los que es clave la movilidad.
- Gestión segura de la información. Además, presenta seguridad de la gestión de la información, ya que existen mecanismos y medidas de seguridad para evitar su interceptación, acceso o alteración por parte de terceros no autorizados. También el sistema es seguro y fiable en cuanto a la generación de alarmas, prefiriéndose un pequeño margen de falsos positivos al riesgo de ignorar un suceso de alarma.

Desde el punto de vista la gestión de residencias y servicio ofrecido este sistema también ofrece importantes mejoras, que se pueden resumir globalmente en los siguientes puntos clave:

- mejora de la calidad de vida de residentes
- mejora de las herramientas de control y monitorización de los eventos y situaciones en la residencia para los trabajadores, facilitando una mayor eficiencia de su trabajo, así como mayor alcance de su servicio.

Estos beneficios críticos se deben, de una manera más detallada, a las siguientes mejoras:

- Gran flexibilidad y escalabilidad a la hora de integrar nuevos servicios, patrones de observación y respuesta y dispositivos inteligentes asociados. A diferencia de la rigidez que ofrecen muchos sistemas propietarios, SAFE-ECH permite una fácil integración de nuevos sensores, sin las restricciones de otros sistemas.

- Tiempo de respuesta reducido. Por un lado el sistema SAFE-ECH responde automáticamente a los estímulos, en contraste a métodos de gestión tradicionales. Por otro lado el sistema puede integrar muchos casos de uso nuevos, que pueden ser configurados de forma muy refinada haciendo uso del CEP, permitiendo una gestión muy eficiente que minimiza tiempos, en comparación con otros sistemas. Por otro lado este sistema proporciona como respuesta ciertas acciones automáticas en lugar de hacerse con mano humana. Si estas acciones dependiesen de un operador serían mucho más costosas en términos de tiempo empleado y costes de personal, ya que normalmente en ese caso el operador se dedicaría exclusivamente a este tipo de tareas.
- Mecanismos de razonamiento personalizados para la operación de la residencia en el ámbito de los residentes y trabajadores, teniendo en cuenta como factores el historial médico o la medicación aplicada, o mecanismos más generalizados para la gestión de la propia residencia como un edificio inteligente teniendo en cuenta sus características especiales.
- Mejora en la gestión de procedimientos y protocolos de actuación. SAFE-ECH permite un mayor control de los eventos y su análisis, permitiendo análisis de combinaciones de factores complejas, además de gran flexibilidad a la hora de establecer los protocolos de actuación y respuesta. Además, su acceso ubicuo desde dispositivos tales como móviles y tabletas permite que los trabajadores sepan las una comunicación de situaciones y acciones a realizar de manera inmediata y temporalmente muy eficiente.
- Aumento de la dignidad de los residentes respecto a servicios de supervisión y cuidados con la utilización de sensores no intrusivos en su vida cotidiana. Esta monitorización con dispositivos IoT y métodos cuidadosamente elegidos para no invadir la intimidad del residente y ser lo menos invasivos posible permite que los individuos tengan mayor independencia, intimidad y un cuidado más rápido y efectivo ante eventos que requieran atención frente al uso de métodos tradicionales o sistemas más invasivos.
- Mejora de la seguridad de los residentes, ya que permite un gran control y monitorización de situaciones que puedan entrañar peligro y una eficiente gestión de alarmas, que llegan automáticamente a los trabajadores. Al permitir la inclusión de un gran número de sensores y de tipo muy variado, además de configurarse de manera muy flexible la gestión dentro del sistema

central, pudiendo analizar y programar respuestas para eventos complejos, se puede cubrir muy eficientemente la monitorización y respuesta a elementos o situaciones que puedan entrañar peligro, e incluso focalizarse en la prevención en muchos casos. Por otro lado, todos los trabajadores tienen acceso a la información de monitorización del sistema y reciben las alarmas a atender inmediatamente.

- Mejorar la calidad asistencial. Por un lado pueden establecerse servicios AAL basados en todo tipo de sensores sin restricciones, pudiendo tener servicios de monitorización y atención muy variados y completos. Por otro lado, los cuidadores tienen un mayor conocimiento de las necesidades específicas en cada momento y de manera inmediata, y muchos procesos son gestionados de manera automática, pudiendo ofrecer sus labores de cuidado de manera mucho más eficaz. Los tiempos de respuesta reducidos contribuyen a una mayor calidad de servicio de atención.
- Gestión simultánea de múltiples residencias, lo que conlleva ventajas para grupos que lleven la gestión de un conjunto de residencias, lo que permite un mejor control y la generación de ciertas sinergias. Esto permite que empresas usuarias que gestionen más de una residencia puedan crear un centro de gestión de nivel superior que comprende una monitorización global y gestión de alarmas centralizadas.
- Reducción de costes. Se estima que el uso de este sistema permite una reducción de costes significativa al poder optimizar procesos, ofrecer una gran extensibilidad y reducir el equipamiento en cada residencia. Además de también, como consecuencia, ofrecer una potencial reducción de costes directos de mantenimiento preventivo y correctivo.

Evaluación desde la perspectiva de la interoperabilidad

En las residencias del grupo bajo estudio se han podido integrar redes de sensores muy heterogéneas. Así mismo, es posible incluir o eliminar fácilmente sensores desde el HMI, indicando su ID y -en caso de inclusión- su tipo y geoposición en el sistema de coordinadas GIS.

Esta integración de sensores dispares se consigue al proporcionar una interfaz de comunicación donde deben enviarse los datos de los sensores, con una definición clara del formato de datos, codificación y estructura a utilizar en los mensajes y operaciones a través del API, ampliamente conocida y documentada. En este sentido

se puede entender que el SOS permite la habilitación de la interoperabilidad técnica de los sensores y actuadores y el sistema completo de adquisición de datos y actuación dentro del sistema SAFE-ECH. Por supuesto, hay otros elementos y factores necesarios para permitir la interoperabilidad técnica de los distintos dispositivos inteligentes y el sistema de gestión, como por ejemplo la existencia de conectividad en el área de la residencia o el gestor de mensajería responsable del envío de la información de sensores al SOS.

El SOS podría ser comparable a una plataforma IoT en el sentido de que recibe los datos de los sensores y a través de su API permite a los usuarios autorizados o al sistema SAFE-ECH acceso a la información en el formato y modelo de información del SOS.

Esta información recibida de los sensores, además, está homogeneizada en un modelo uniforme para observaciones y no sigue una multitud de formatos y modelos de datos dispares de los distintos sensores con un soporte muy parcialmente diseñado e insuficiente para este tipo de información a la hora de incluir nuevos campos relevantes o tipos de medidas. Esto permite la consecución de niveles superiores de interoperabilidad.

Por tanto, se puede concluir que los objetivos de trabajo de investigación realizado se han conseguido satisfactoriamente. Ha sido posible la habilitación de interoperabilidad a diferentes niveles mediante el seguimiento de estándares comunes y el uso de un Servicio de Observación de Sensores. Siguiendo estándares abiertos y utilizando una implementación del SOS del OGC se ha podido integrar redes de sensores heterogéneos en este sistema AAL para gestión de residencias, con independencia de su tipo, marca o tecnología de comunicación asociada. Por otro lado, también se han integrado la gran variedad de tipos de mensajes que estos sensores generan, conteniendo información de monitorización de la residencia. La representación de estos datos IoT ha sido homogeneizada tanto sintácticamente (formato de datos) como a nivel de codificación y estructura (siguiendo las codificaciones del OGC O&M en el caso de las observaciones y SensorML en el caso de sensores y actuadores), habilitando la interoperabilidad sintáctica de la información y sentando las bases para el establecimiento de la interoperabilidad semántica. Hay que notar que esta estructura es capaz de soportar y representar el tipo de información IoT proporcionada por sensores de una manera extensiva y genérica, evitando pérdida de información y ambigüedad. Con el diseño y definición

de un vocabulario conteniendo los distintos términos y conceptos necesarios para registrar esta información IoT de monitorización de residencias en los modelos O&M y SensorML se ha conseguido el último requisito necesario para poder habilitar la interoperabilidad semántica de la información. De esta manera, los datos IoT representados con este modelo semántico pueden ser entendibles y utilizables automáticamente entre todos sistemas que utilicen este estándar de información (incluyendo el vocabulario común) y accedan a la información de sensores a través de la interfaz del SOS.

Por último, el sistema de gestión permite la integración de múltiples residencias, y su gestión individual o múltiple, creando un sistema de sistemas en el que está habilitada la interoperabilidad semántica entre ellos. El modo de gestión múltiple o multirresidencia permite utilizar automáticamente información de cada sistema de gestión local proporcionando un panel de alarmas global e información específica de cada una de ellas. Esto constituye un claro ejemplo de interoperabilidad semántica entre sistemas.

Como ya se destacó en la introducción, el caso general entre sistemas IoT es la heterogeneidad, especialmente a nivel semántico, y como posible solución para poder permitir la interoperabilidad y el entendimiento de la información debe proporcionarse a estos sistemas un modelo de información común, además de, a ser posible, alicientes y facilidades para su implementación.

El uso de un modelo consolidado y ampliamente conocido, con una gran comunidad de desarrolladores e investigadores respaldándolo, es un aliciente importante para su adopción y su futura aceptación por parte de otros sistemas. El hecho de que ya esté implementado en un Servicio de Observación de Sensores de código abierto y disponible, y en el sistema de gestión que incorpora. Por otro lado la flexibilidad y usabilidad del sistema, y sus otras ventajas frente a sistemas de gestión propietarios existentes, favorecen su implantación y el uso de este modelo de información asociado.

4.8. Conclusiones y perspectivas futuras

En este capítulo se ha descrito un sistema desarrollado, SAFE-ECH, diseñado como una solución tanto AAL como AMI para el soporte de AHA, que sigue los estándares abiertos OGC. En este sentido, se beneficia de un estándar interno y de un acceso

fiable a la información de monitorización de los sensores, de un sistema de alerta fiable y de un soporte de datos geoespaciales que permite funcionalidades de localización. Estas funcionalidades permiten la creación de servicios innovadores y muy útiles en el contexto de la Vida Asistida, y la mejora de los existentes mediante el avance de información geoespacial adicional.

SAFE-ECH es un sistema basado en código abierto que incorpora servicios dentro del marco SWE. SAFE-ECH tiene como objetivo maximizar el confort, la seguridad y la eficacia y eficiencia del servicio para las personas mayores en las residencias a través de la vida asistida. Para ello, utiliza un conjunto de sensores y actuadores para recopilar información relevante, aplica un análisis inteligente de datos para decidir y realizar las mejores acciones del curso y proporciona a los cuidadores una Interfaz Hombre-Máquina para facilitar la gestión y monitorización de las residencias. El SOS de la especificación SWE es un elemento clave del sistema para integrar y recuperar los datos generados por la colección de sensores que representan las fuentes de información del entorno de Inteligencia Ambiental que crea el sistema.

Este sistema proporciona una completa flexibilidad en varios niveles: integración y configuración de sensores, reglas de gestión y actuación, y servicios para los ancianos. Por lo tanto, puede adaptarse a cualquier residencia, y también podría extenderse a otros entornos como las residencias de ancianos.

Las principales funcionalidades del sistema han sido validadas no sólo desde un ámbito teórico, sino también en la práctica ya que SAFE-ECH ha sido desplegado en residencias reales en España, cubriendo una amplia gama de servicios AAL como localización, control de acceso, alarma de fuga, alarmas médicas y de emergencia, detección de intrusos, control de pañales, y otros. La localización y otros servicios basados en el seguimiento, así como los anteriores servicios que se mejoran de alguna manera mediante el uso de la información de geolocalización, son posibles gracias al uso del soporte geoespacial.

Una potencial línea de investigación futura es el uso de una implementación ligera del SOS en nuestro sistema, como SOSLite [159], que permitirá una transmisión y un procesamiento de datos de forma notablemente más rápida y ligera. Esta variación del sistema será óptima para entornos especiales en términos de optimización de recursos, y previsiblemente aportará beneficios derivados de esta ventaja. Otro tipo de mejora potencial prevista sería el incremento de la funcionalidad del sistema, integrando nuevos casos de uso, y la integración del sistema con los servicios públicos

de emergencia para disminuir el tiempo de reacción ante cualquier emergencia médica.

Por otro lado, este sistema también podría ser adaptado con relativa facilidad a otros entornos IoT fuera del ámbito de residencias, ya que la estructura es apta para la gestión inteligente de redes de sensores IoT en muchos otros ámbitos de aplicación.

Fuera del ámbito de gestión de residencias, se podría implementar en sistemas IoT que decidan adoptar los estándares OGC para la gestión de sus datos, y opten por su uso para proporcionar una gestión inteligente de la información IoT recogida. Para ello sería necesario una adaptación de los servicios proporcionados. Se estudia su inclusión futura en Hogares Inteligentes (especialmente en los orientados al cuidado y seguridad de la tercera edad) y en hospitales.

Desde el punto de vista de la interoperabilidad, notablemente el uso del SOS permite la integración de redes de sensores heterogéneos, permitiendo salvar esta barrera de la interoperabilidad técnica. También habilita la interoperabilidad sintáctica al definir el formato de datos en que debe estar representada la información. La consecución de la interoperabilidad en estos sistemas IoT, un reto técnico general en IoT muy complejo, se consigue aplicando el uso de estándares e interfaces comunes, homogeneizando la representación, acceso e intercambio de información. Mediante el uso de los estándares (estructura y codificación) del marco SWE del OGC y un vocabulario común para referenciar los tipos de sensores, magnitudes, lugares y características de interés, se permite la interoperabilidad semántica tanto intra como inter-sistema. Como ya se ha remarcado en la evaluación desde el punto de vista de interoperabilidad, se han cubierto todos los objetivos de investigación de este trabajo en el marco de esta tesis doctoral.

Por último, desde el punto de vista de la digitalización de nuestro mundo, este sistema, así como el SOS que integra, constituye un habilitador digital que impulsa la transformación digital de las residencias. Hay que destacar que convierte en cierta medida a la residencia en un entorno AMI y también crea su gemelo digital. Pero no solo impulsa la digitalización al crear un gemelo digital de la residencia, sino que también facilita mucho la transformación digital de estos entornos:

- al permitir la integración de cualquier conjunto de sensores, independientemente del tipo de sensores o sistemas de adquisición de datos

que se empleen, permitiendo la integración de más tipos de servicios y favoreciendo su

- al permitir inclusive si había sistemas de gestión IoT AAL rudimentarios, obsoletos o cerrados ya implantados en la residencia, su integración en SAFE-ECH permitiendo su crecimiento flexible y evolución con la adopción de nuevos servicios, dispositivos y capacidades de gestión que no se podrían conseguir con los sistemas rígidos anteriores. Esto podría pasar con por ejemplo con sensores que simplemente activan una alarma y no tienen plataforma de gestión, o bien un sistema cerrado de gestión que ya no satisface sus necesidades o no es capaz de explotar el potencial AAL de los dispositivos actuales.
- al permitir la escalabilidad y flexibilidad de soluciones y servicios AAL. De hecho, que esto pueda ser así es un gran aliciente para su implantación y transformación digital
- al proporcionar gran usabilidad, lo que facilita su adopción y uso, especialmente en entornos no tradicionalmente técnicos
- al permitir la interoperabilidad a varios niveles entre sistemas afines que utilicen estándares abiertos del SOS o bien entre sistemas SAFE-ECH, que además pueden generar sinergias entre ellos, y constituye un aliciente para su adopción, iniciando o continuando la transformación digital
- al permitir la interoperabilidad entre residencias de manera flexible, permitiendo la gestión de un sistema-de-sistemas, llevando la transformación digital a un nivel superior
- al permitir el crecimiento futuro del sistema de gestión en aplicaciones por encima o módulos complementarios, ya que facilita la creación de estos por su uso de estándares abiertos, módulos y aplicaciones, ya sea creadas para otros sistemas, adaptando ligeramente otras creadas, o diseñadas específicamente, lo que es más fácil que ocurra y se realice de forma poco costosa y sencilla al tener unos estándares de referencia

Y dada su posible aplicación en un futuro en otros campos, no solo impulsa la Residencia Digital y la creación de gemelos digitales de estos centros, sino que también puede potencialmente promover la transformación digital en otros ámbitos como Hogares Inteligentes para 3º Edad o gestión AAL de hospitales o bien subdominios concretos de la gestión hospitalaria.

CAPÍTULO 5

Interoperabilidad semántica entre plataformas heterogéneas

"Toda la Tierra hablaba una misma lengua y usaba las mismas palabras [..]

Pero Yaveh [..] vio la ciudad y la torre que los hombres estaban edificando y dijo:
«He aquí que todos forman un solo pueblo y todos hablan una misma lengua; siendo este el principio de sus empresas, nada les impedirá que lleven a cabo todo lo que se propongan.

Pues bien, [..] confundamos su lenguaje para que ninguno entienda el habla de su compañero, de modo que no se entiendan los unos con los otros».

Así, Yahveh consiguió que cesasen de trabajar juntos [..].
Por ello la ciudad se la llamó Babel."

La Torre de Babel, Génesis

5.1. Introducción

Como ya se ha visto, el ecosistema global IoT está fragmentado y proliferan silos verticales de información aislada por dominio de aplicación. Esto se debe a la falta de interoperabilidad de la información entre las plataformas IoT, debido a su gran heterogeneidad a muchos niveles. En concreto, la falta de interoperabilidad semántica se debe en gran medida a los distintos modelos de representación de la

información que utilizan las plataformas, que suele ser distinto para cada instancia concreta de plataforma.

Las soluciones basadas en el uso de estándares comunes son difícilmente aplicables al conjunto de plataformas heterogéneas que conforman el ecosistema global de IoT. Por lo general solo son aplicables en la fase de diseño de un sistema IoT. Más adelante, resulta muy costoso o no viable el cambio de estándares, modelos de información o la modificación de interfaces en una plataforma. A falta de un estándar global al que la gran mayoría de sistemas y plataformas estén alineados, hay una gran necesidad de otro tipo de soluciones de interoperabilidad para habilitarla entre plataformas y sistemas heterogéneos, y muy especialmente en el caso concreto de los modelos de información. El reto más arduo en IoT es términos de interoperabilidad es la interoperabilidad semántica de la información entre plataformas heterogéneas cuando se utilizan modelos semánticos de información diferentes. Actualmente, fuera del uso de un modelo semántico común entre ellas (alineación por el uso de ontologías, siguiendo por tanto un estándar en modelos de información afín) hay un gran vacío que cubrir en la literatura.

En este capítulo se estudia un conjunto de soluciones de interoperabilidad a todos los niveles de un sistema IoT y entre sistemas heterogéneos, creados desde un enfoque nuevo e innovador dentro del marco del proyecto H2020 INTER-IoT. Estas soluciones innovadoras siguen un enfoque diferente al uso de estándares comunes para lograr la interoperabilidad, en concreto todas ellas efectúan adaptación de elementos para habilitarla. Muy notablemente, son capaces de proporcionar interoperabilidad semántica entre plataformas heterogéneas con modelos de información dispares, mediante el uso del único traductor semántico para IoT existente, salvando esta gran barrera de interoperabilidad y abriendo un horizonte de posibilidades en el actual ecosistema global IoT.

En el marco de esta tesis doctoral se ha participado en el proyecto de investigación INTER-IoT, contribuyendo en diversas tareas de ámbito general junto con otros miembros del consorcio, así como de manera más particular en las contribuciones mencionadas de manera específica a lo largo del capítulo.

5.2. Enfoque para la interoperabilidad de INTER-IoT

A diferencia de las soluciones de interoperabilidad basadas en el uso de estándares comunes, alineando los sistemas para que sean afines y similares, el proyecto INTER-IoT ha diseñado soluciones de interoperabilidad para sistemas que no son afines, y resultan muy distintos y heterogéneos (el caso general en IoT) [39][29].

Para su diseño y desarrollo, se ha llevado a cabo un enfoque de adaptación de elementos (semántica, formatos de datos, protocolos de red..) en lugar tratar de conseguir uniformidad del elementos, como es el caso de la alineación de estándares. Este enfoque es más complejo que la simple adherencia a un estándar, en que los sistemas simplemente tienen que ser construidos siguiendo un modelo establecido. Una solución de interoperabilidad entre sistemas y elementos heterogéneos implica el añadido el estudio y manejo de varios modelos, en lugar de uno solo, el estudio y diseño de formas de adaptarlos y transformarlos, y la creación de elementos de adaptación. Además, también implican solventar el importante reto de tener que gestionar la adaptación de los grandes flujos de datos e información (IoT Big Data) en tiempo real. También, la heterogeneidad de los elementos a adaptar implica una gran complejidad en términos de diseño y desarrollo para poder realizar una adaptación potencial.

Pero en cambio, puede aportar soluciones a problemas de interoperabilidad que no pueden solucionarse con la estrategia de uso de estándares comunes. Los sistemas heterogéneos difícilmente pueden ser modificados para encajar con estándares diferentes. INTER-IoT en este sentido no tiene como objetivo homogeneizar los sistemas, sino diseñar soluciones no invasivas que no implican la modificación interna de sistemas y plataformas IoT.

Las soluciones de interoperabilidad de INTER-IoT serían un elemento intermedio entre sistemas y plataformas IoT heterogéneas que aportaría interoperabilidad entre ellas, capa a capa (dispositivo, red, middleware, aplicación y semántica). Por otro lado, a nivel de dispositivo, red y aplicación la interoperabilidad puede ser intra-capa, es decir, dentro de un mismo sistema IoT, en capas que están asociadas a una sola plataforma [39][8].

También ha seguido un enfoque con especial atención a las necesidades de interoperabilidad de las capas, orientado a buscar soluciones de interoperabilidad a cada capa de manera individual para así lograr una interoperabilidad muy completa y precisa en ella, a diferencia de lo que se suele conseguir con enfoques más globales, que suele resultar una solución parcial. Pero a su vez, también permite una interoperabilidad global al combinar de manera flexible las soluciones individuales en cada una de estas capas.

Además, su objetivo también es habilitar la interoperabilidad entre plataformas heterogéneas, el mayor reto de interoperabilidad en IoT. De esta manera propone un enfoque para conseguir la interoperabilidad en las capas de un sistema, a través de las capas de un sistema, y a la vez entre distintas plataformas y sistemas heterogéneos [8].

5.3. Arquitectura Multicapa de Interoperabilidad

En el proyecto H2020 INTER-IoT se ha diseñado una novedosa arquitectura de interoperabilidad multicapa, con el fin de proporcionar interoperabilidad de manera eficiente y muy precisa en cada una de las capas de un sistema IoT, y de manera global en el conjunto de todas ellas, además de poder establecerla entre distintos sistemas y plataformas IoT heterogéneas. Las capas consideradas serían dispositivo, red, middleware, semántica y aplicación y servicios.

Esta arquitectura es el resultado del trabajo conjunto del consorcio de INTER-IoT. En el marco de esta tesis doctoral se ha participado y contribuido principalmente en el área de la interoperabilidad semántica en lo referente a ella. Además, se ha contribuido en la identificación, descripción, catalogación y cribado de requisitos técnicos funcionales y no funcionales y en tareas generales dentro de los paquetes de trabajo de desarrollo y de arquitectura.

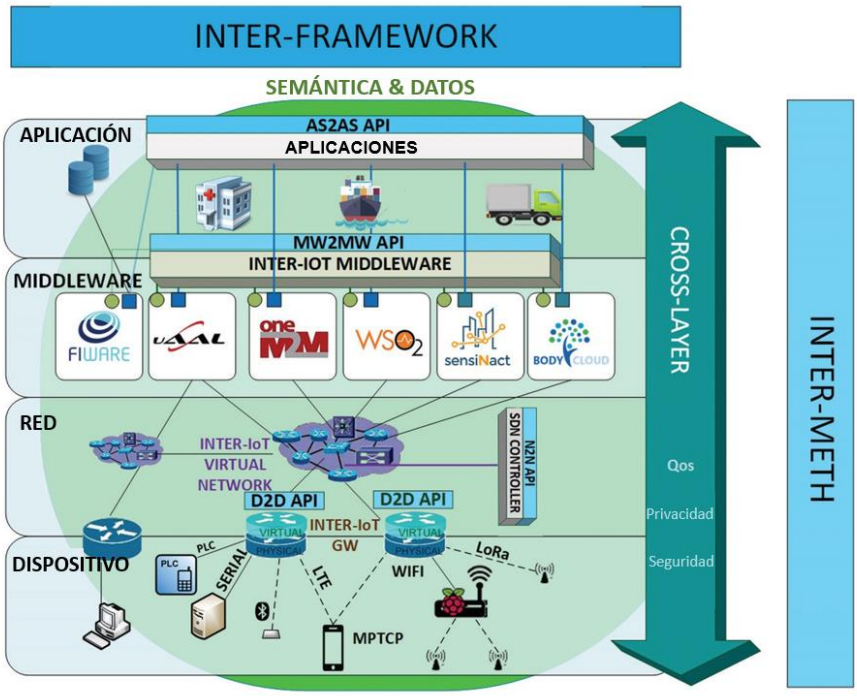


Figura 5.1 Arquitectura de interoperabilidad multicapa de INTER-Io

Esta arquitectura está compuesta por tres bloques principales interrelacionados:

- -INTER-LAYER [39]: un conjunto de herramientas específicas, que permiten habilitar la interoperabilidad en los sistemas IoT heterogéneos. INTER-LAYER proporciona una herramienta específica en cada capa de un sistema IoT para cubrir sus necesidades específicas de interoperabilidad en ella. Estas herramientas se pueden utilizar de forma flexible, en cada capa en la que se quiera utilizar o no
- -INTER-FW [182][39]: un framework de integración de soluciones, es decir, un programa con interfaz gráfica que integra todas las herramientas de INTER-LAYER y ofrece algunas funciones extra de monitorización. Su fin es proporcionar una herramienta para gestionar y monitorizar el uso de las soluciones de interoperabilidad utilizadas sobre un sistema o sistemas IoT de

forma fácil y usable, desde una interfaz gráfica, facilitando la labor a gestores y programadores.

- -INTER-METH [34]: una metodología para la implementación de una o varias soluciones de interoperabilidad genéricas en sistemas reales, pudiendo realizar su particularización a las características concretas y particulares. La implementación de soluciones requiere realizar despliegues determinados de software, una configuración correcta teniendo en cuenta las características del caso de aplicación real, e inclusive puede requerir el desarrollo de una pieza de software determinada (puente o alineamiento) que debe integrarse en determinadas herramientas.

Las soluciones de interoperabilidad de INTER-IoT serían un elemento intermedio entre sistemas y plataformas IoT heterogéneas que aportaría interoperabilidad entre ellas, capa a capa. Por otro lado, a nivel de dispositivo, red y aplicación la interoperabilidad puede ser intra-capa, es decir, dentro de un mismo sistema IoT, en capas que están asociadas a una sola plataforma.

5.3.1. INTER-LAYER: conjunto de soluciones de interoperabilidad capa a capa para sistemas IoT

Los sistemas IoT gestionados por plataformas heterogéneas tienen diferentes necesidades de interoperabilidad en cada nivel o capa. Dentro del proyecto se han diseñado herramientas para cada capa, que permiten habilitar la interoperabilidad en ella.

Se pueden instalar y utilizar de manera independiente, y elegir de manera flexible qué conjunto de ellas aplicar en un sistema o sistemas IoT heterogéneos gestionados por plataformas IoT. Todas ellas exponen una interfaz (API REST) para su configuración y explotación, que puede ser utilizada por capas adyacentes. Muy notablemente, pueden unir las capas de distintos sistemas y plataformas IoT, permitiendo la interoperabilidad sin barreras entre ellas, y solucionando uno de los problemas de falta de interoperabilidad en IoT más arduos y limitantes: la interoperabilidad entre

plataformas IoT heterogéneas, que no siguen los mismos estándares, formatos, modelos de información y semántica.

Pueden permitir la interoperabilidad en capas concretas de sistemas IoT heterogéneos, y a la vez de manera global, mediante el conjunto de todas ellas o un grupo de ellas. Además, de manera muy notable, permiten la interoperabilidad entre sistemas gestionados por plataformas IoT heterogéneas capa a capa.

Cada una de estas herramientas constituye un habilitador de interoperabilidad para plataformas IoT (a distintos niveles del sistema IoT), y por sí consituye un habilitador digital que favorece e impulsa la digitalización de este mundo.

Estas herramientas son de código abierto y están disponibles en línea [183]. Además, también cuentan con una versión virtualizada mediante tecnología docker también disponible que puede ser levantada instantáneamente con independencia del sistema operativo y del entorno.

Notablemente, entre estas herramientas altamente innovadoras está el único traductor semántico para IoT existente actualmente [35], capaz de proporcionar interoperabilidad semántica entre plataformas IoT heterogéneas, permitiendo el intercambio y la comprensión de información entre silos verticales, y representando por tanto una solución de interoperabilidad a uno de los desafíos más complejos en IoT.

5.3.1.1 *Dispositivo*

Esta capa está compuesta por los objetos inteligentes (sensores, actuadores y dispositivos virtuales) en un sistema o plataforma IoT, los cuales a menudo tienen recursos computacionales, energéticos y memoria limitados[6].

Las necesidades de interoperabilidad de esta capa son la posibilidad de poder establecer comunicación y enviar datos a una plataforma IoT, a la nube, a servicios en una capa superior o entre dispositivos IoT. En general los dipositivos de capacidades limitadas no pueden hacerlo directamente sin la ayuda de un elemento intermedio, ya que su capacidad de conectividad es muy limitada (generalmente utilizan

tecnologías de comunicación de corto alcance y baja potencia) y no pueden conectarse a la red, como tampoco hacer las conversiones de protocolo o preprocesar los datos.

La solución proporcionada en INTER-LAYER para cubrir estas necesidades de interoperabilidad en la capa de dispositivo es una pasarela de red inteligente que permite la conexión de dispositivos IoT de bajos recursos que utilicen tecnologías de comunicación de corto alcance y baja potencia (ej. Bluetooth).
Esta necesidad se puede cubrir con una pasarela inteligente IoT de red, que habilita las comunicaciones D2G (dispositivo con la pasarela), D2C (dispositivo con la nube, plataforma o servicio en un nivel superior) y D2D (objeto IoT con otro objeto IoT, lo que no suele ser directamente posible). Estas pasarelas requieren de muchas más capacidades y funcionalidad que las pasarelas de red comunes, ya que deben proporcionar conectividad a tecnologías inalámbricas IoT de corto alcance, y realizar servicios de procesado de datos y conversión de protocolos.

Esta pasarela [184] está dividida en dos partes: una física y una virtual, conectadas a través de la red, y combina las soluciones para las necesidades de interoperabilidad de los dispositivos, así como las necesidades de interoperabilidad con el uso de redes, que se ve seguidamente. La parte física que sólo maneja el acceso a la red y los protocolos de comunicación, mientras que la parte virtual que maneja todas las demás operaciones y servicios de la pasarela. La pasarela sigue un enfoque modular para permitir la adición de bloques de servicio opcionales, para adaptarse al caso específico.

Soporta nuevos protocolos especialmente diseñados para IoT como CoAP y distintas y la conexión a ella mediante distintas tecnologías de comunicación típicas de dispositivos IoT tales como ZigBee y Bluetooth, así como WiFi. Además, la parte virtual soporta distintos servicios para cubrir las necesidades de interoperabilidad de la siguiente capa de un sistema IoT, el nivel de red.
Hay que destacar, desde el punto de la interoperabilidad intra-capa, que uno de los objetivos de diseño es poder conseguir la interoperabilidad entre dispositivos (D2D), es decir, entre dos dispositivos inteligentes heterogéneos, que generalmente no son capaces de poder comunicarse directamente entre ellos. La pasarela de INTER-IoT, o

solución D2D, permite que dispositivos IoT conectados a ella sean capaces de establecer comunicación entre ellos.

Por tanto, esta pasarela proporciona interoperabilidad técnica a los objetos inteligentes conectados a ella (D2G), permitiéndoles comunicarse con otros dispositivos (D2D) o con una plataforma IoT o servicios en un nivel superior (D2C).

5.3.1.2 ***Red***

La capa de red de un sistema IoT está compuesta por el conjunto de redes entre los objetos IoT y la capa de plataforma, middleware, la nube u otros servicios, a través de las cuales se envían los datos IoT. Conceptualmente comprendería el conjunto de protocolos, sistemas y dispositivos que funcionan en el nivel de red de la pila de protocolos OSI. Esta capa contiene elementos de hardware como conmutadores, cortafuegos, enrutadores y puentes, e incluye a las denominadas redes IoT (desde la nube de objetos inteligentes a la pasarela) que son significativamente diferentes de las redes tradicionales y suelen tener capacidades limitadas [6].

Las redes tienen necesidades de interoperabilidad y problemas de recursos y conectividad específicos. Actualmente, el tráfico en la red con la llegada de Internet de las Cosas está creciendo exponencialmente año tras año, y se necesitan soluciones para optimizar la capacidad y uso de las redes. La inmensa cantidad de flujos de tráfico generados por los dispositivos inteligentes es extremadamente difícil de manejar, y la escalabilidad de los sistemas IoT es difícil debido en buena parte a las limitaciones de las redes y su falta de flexibilidad. También, con la llegada del Internet del Futuro, trayendo por ejemplo las redes móviles 5G, es necesario tener herramientas para poder explotar sus grandes capacidades [11].

Uno objetivo de interoperabilidad intra-capa es poder conseguir interoperabilidad entre redes (N2N), entendiéndose por la posibilidad de unir redes separadas físicamente como si fueran una sola o la itinerancia transparente de objetos. Otro problema o necesidad de interoperabilidad es la movilidad transparente de objetos inteligentes a través de diferentes redes.

El uso de los paradigmas SDN [98](Redes Definidas por Software, que permiten un gran control sobre su gestión) y NFV(Virtualización de Funciones de Red) [185] puede

aportar soluciones a estos problemas y necesidades mediante la creación y gestión de redes virtuales. En este sentido, la parte virtual de la pasarela INTER-IoT ofrece funcionalidades y soporte para el uso de SDN y NFV. La pasarela permite la interoperabilidad N2N mediante la creación de una red virtual SDN, controlada desde su API N2N, utilizando tecnologías como el protocolo OpenFlow, OpenVSwitch y un controlador flexible. También permite el uso de los paradigmas SDN y NFV para construir soluciones sobre ellos que mejoren la gestión del tráfico o la explotación de capacidades 5G.

5.3.1.3 *Middleware*

Un middleware es un software permite el flujo de información entre los objetos inteligentes y las aplicaciones que quieren interactuar con ellos y utilizar la información IoT que generan. Un middleware proporciona una capa de conectividad para sensores, actuadores, y redes de sensores; por otro lado, también proporciona una interfaz de conectividad para las aplicaciones que desean recibir datos de los sensores, o realizar cualquier otra interacción con ellos [186]. Un middleware forma parte de una plataforma IoT y proporciona servicios que garantizan una comunicación eficaz entre esos elementos, permitiendo así la interoperabilidad entre ellos [18].

Las necesidades actuales de interoperabilidad a nivel de middleware son [187]:

- el descubrimiento de sensores, gestión de la información de los objetos conectados. El middleware de por sí es un habilitador de interoperabilidad entre los torrentes de datos fluyendo en tiempo real de los sensores entre sensores, actuadores y la plataforma IoT.
- la interconexión y flujo de información entre plataformas IoT heterógeneas

La solución desarrollada para cubrir estas necesidades de interoperabilidad, llamada Inter-MW, es un middleware capaz de integrar otros middlewares, permitiendo la integración horizontal de plataformas heterogéneas e interoperabilidad sintáctica entre ellas.
Sus principales funciones son la gestión de la comunicación entre plataformas, las funciones de gestión de recursos típica de un middleware y la adaptación sintáctica

de los formatos de datos, transformando la información a un formato sintáctico común, como típicamente hace el middleware de una plataforma. El formato en que gestiona la información proveniente de sensores el middleware, y la proporciona a las aplicaciones y servicios a través de su API es JSON-LD. A diferencia de los middlewares de plataforma, Inter-MW debe gestionar la comunicación con las plataformas. Para ello debe interactuar con el API de cada plataforma, teniendo en cuenta las especificaciones de su interfaz y tipo de inputs y respuestas específicas, y modo de gestión de información que son distintas en cada tipo de plataforma. Entre estas características se incluiría el formato de datos en que se obtiene la información. Por ello, es necesario desarrollar un módulo de comunicación específico para gestionar la comunicación con cada tipo de plataforma particular (ej. FIWARE, universAAL, etc), llamado puente de comunicación con la plataforma. La comunicación con plataformas y se hace por medio de un gestor de mensajería con el procedimiento publicador-suscriptor, y se puede gestionar y configurar la publicaciones y suscripciones desde el API del middleware. Otras entidades como aplicaciones o usuarios que quieran obtener esta información IoT, pueden suscribirse a ella de la misma manera.

Como middleware, tiene las siguientes funciones: registro de dispositivos, registro de plataformas, gestión de dispositivos (incluyendo virtuales), descubrimiento de dispositivos IoT conectados a las plataformas, gestión observaciones y actuaciones, gestión plataforma, modificación o eliminación de dispositivos, eliminación de plataforma.

Permite de esta manera no solo la comunicación entre plataformas, dispositivos y aplicaciones, sino también la comunicación entre plataformas.

Inter-MW [188] facilita la interoperabilidad sintáctica entre plataformas heterogéneas de IoT, así como la gestión interna de la información de un middleware, pero aunque proporciona un formado de datos común para la información proveniente de las plataformas y dispositivos, no sucede así con el modelo de datos o modelo semántico, que sigue siendo el propio de cada plataforma. Por tanto, no llega a habilitar la interoperabilidad semántica entre plataformas

La interoperabilidad en el nivel de middleware se consigue mediante el establecimiento de una capa de abstracción y la vinculación de las plataformas IoT a ella. Los diferentes módulos incluidos en este nivel proporcionarán servicios para

gestionar la representación virtual de los objetos, creando la capa de abstracción para acceder a todas sus características e información

Respecto a la seguridad que ofrece como herramienta, Inter-MW soporta OAuth 2.0, y aparte, soporta seguridad básica, autenticación, conexión segura e integración con gestores de identidad y autenticación SSO.

5.3.1.4 *Aplicaciónes y Servicios*

En esta capa está el conjunto de aplicaciones y servicios que requieren información IoT de la capa de dispositivos para la función que realizan, y la reciben a través de una plataforma IoT (es decir, en el formato sintáctico y modelo de información de esta plataforma, interactuando con su interfaz REST API).

Se proporcionó una herramienta gráfica (AS2AS) [189][39] que permite el fácil reuso, combinación y orquestación de aplicaciones y servicios heterogéneos, los cuales pueden provenir de varias plataformas IoT distintas y utilizar datos IoT de ellas (cada aplicación puede estar asociada a una sola plataforma, salvo muy raras excepciones).

Esta herramienta, basada en la herramienta de código abierto Node-RED [190], está fundamentada en el paradigma “flow-based” o basado en flujo, que interpreta las aplicaciones como una caja negra con interfaces de entrada y salida. Estas cajas negras se pueden combinar, reusar y orquestar temporalmente creando un flujo de ejecución con tiempos perfectamente definidos, importando las aplicaciones o cajas negras a usar y conectando adecuadamente sus entradas y salidas de manera orquestada (directamente o utilizando elementos adaptadores o temporales entre ellas). Esta combinación de flujos entre entradas y salidas en nodos (aplicaciones, REST APIs, elementos adaptativos o elementos de gestión temporal) constituye un diagrama de flujo AS2AS que puede ser almacenado como un fichero en el programa, modificable posteriormente, y puede ejecutarse llevando a cabo la secuencia de acción.

De esta manera se proporciona una interfaz gráfica de muy alta usabilidad, que facilita en muy alto grado la creación de un flujo de aplicaciones combinadas y orquestadas, que puede incluir elementos adaptadores, de disparo de tiempos o también nodos que representen APIs de servicio de plataformas IoT, u otras APIs accesibles en línea.

Además, proporciona una visión del flujo de manera gráfica y global y su versión virtualizada requiere tan solo segundos en ser levantada, sin requerir un entorno determinado, lo que añade aún mayor usabilidad. Expone un API pero la creación y gestión de flujos se hace generalmente a través de la interfaz gráfica.

Por supuesto, es posible crear un flujo de aplicación orquestado combinando aplicaciones y servicios y con una secuencia de acción clara sin una herramienta de ayuda como esta, pero hacerlo manualmente ad hoc sería muy significantemente más complejo, difícil y engorroso, especialmente en la creación de elementos intermedios entre las aplicaciones o en el enlace entre aplicaciones (lo que conllevaría en ambos crear y levantar numerosos servicios web), además de tener que resolver la gestión temporal.

Se puede considerar que AS2AS es una solución capaz de ofrecer una capa de abstracción que proporciona interoperabilidad entre las aplicaciones y los servicios de las plataformas de IoT, y que permite las siguientes funcionalidades: el acceso, el uso, la importación, la exportación, el registro de datos, el descubrimiento, la combinación y la orquestación de servicios heterogéneos entre diferentes plataformas de IoT. Además, permite la gestión de diagramas de flujo (creación, diseño, almacenamiento, modificación y ejecución), de nodos (creación, almacenamiento, importación y exportación, reuso) y ofrece una visión global gráfica de toda la orquestación.

5.3.1.5 *Capa de semántica y datos*

La capa de semántica y datos comprende a los modelos de información utilizados en los distintos niveles de sistemas y plataformas IoT, y es una capa o dimensión transversal a estos.

Hay una gran necesidad de interoperabilidad semántica entre plataformas IoT heterogéneas, que generalmente representan silos verticales de información no interoperable con otros sistemas, en el sentido de que no es entendible por otros al usar modelos de información distintos [73].

La mayor barrera para este tipo de interoperabilidad semántica es la gran heterogeneidad en los modelos semánticos de información de las distintas instancias

de plataformas IoT que gestionan datos de sistemas IoT concretos. Es importante notar, en términos de heterogeneidad, que cada instancia concreta de un tipo de plataforma IoT por lo general tiene un modelo de información particular, distinto al de otras instancias de esa plataforma, o de otros tipos de plataforma. Esto implica que las distintas plataformas heterogéneas (refiriéndose a instancias individuales) no pueden entender la información proveniente de otras, impidiendo intercambios de información entre ellas. También estas limitaciones se extienden al nivel de la capa de aplicaciones y servicios, ya que las aplicaciones que utilizan datos IoT son específicas para el modelo de datos de la plataforma.

La solución de INTER-IoT para la capa de datos y semántica permite cambiar el modelo semántico en que está representada la información por otro distinto mediante una traducción semántica en tiempo real de ontología a ontología. La información traducida sería la misma en contenido y significado, pero estaría representada mediante otro modelo de información semántico.

Esto es posible mediante el uso de un traductor semántico, el IPSM [44] (Mediador Semántico Entre Plataformas). Este mediador es el único traductor semántico para IoT existente actualmente [191], hasta el punto de que las únicas dos opciones que se aprecian en artículos de revisión de interoperabilidad semántica es el uso de ontologías, creando un modelo semántico común en varios sistemas, o el uso del IPSM [35].

El componente mediador (IPSM) es capaz de realizar las traducciones de ontología a ontología de la información intercambiada utilizando alineamientos semánticos entre las dos ontologías. La traducción semántica es una técnica innovadora. Hay que apreciar que esta gestión y traducción de la información se hace en tiempo real, siendo el traductor un elemento intermedio entre dos plataformas, que no debe inducir ningún retraso significativo para las aplicaciones o la plataforma que reciba y utilice estos datos. Aparte, el IPSM debe ser capaz de gestionar y soportar el uso de datos masivos proveniente de plataformas [44].

El Mediador Semántico Entre Plataformas IoT (IPSM) gestiona los mapeos semánticos entre la plataforma emisora y la receptora, proporcionando interoperabilidad semántica a través de la traducción entre las diferentes ontologías o modelos semánticos de las plataformas IoT que quieren interoperar. Esta traducción se basa

en el uso de alineaciones semánticas, que representan las equivalencias y reglas para realizar traducciones semánticas entre dos entidades diferentes. Estos alineamientos deben haber sido definidos, programados y almacenados en el IPSM previamente. La traducción semántica que efectúa el IPSM permite la transformación de un sistema de información. Al igual que Inter-MW, el IPSM gestiona la información en formato JSON-LD [174], capaz de soportar anotaciones semánticas.

Tiene una REST API que expone operaciones de creación y gestión de canales de traducción, gestión de alineamientos, y opción de traducción en modo mensaje a mensaje en lugar de como flujo de datos.

Más información sobre esta solución de interoperabilidad semántica se puede encontrar en un apartado dedicado a ella, dada su particular relevancia en el paradigma IoT como solución potencial para integrar silos verticales y habilitar un ecosistema IoT horizontal, sin fragmentación por dominios o plataformas, además de otras posibilidades remarcables.

5.3.1.6 *Aspectos transversales a todas las capas o "capa transversal"*

Se considera que hay una necesidad de aspectos no funcionales transversales a todos los niveles de un sistema IoT, y que hay que garantizar especialmente con el uso de las herramientas de interoperabilidad y con los intercambios y flujos de datos a través de ellas. Su objetivo es garantizar aspectos no funcionales que se requieren en todas las capas, como la privacidad, la seguridad, la calidad del servicio y la confianza. Diferentes elementos y mecanismos para ello se han integrado en cada herramienta individualmente y, además, en el framework de integración. En el marco de esta tesis doctoral se diseñó el macropatrón de seguridad combinando TLS, autenticación y gestión de tokens para la protección de las APIs de las herramientas en el framework.

5.3.2. Inter-FW: framework de integración de soluciones

Todas las soluciones de INTER-LAYER se han integrado en un mismo framework (INTER-FW) con el fin de facilitar su gestión, control y monitorización mediante un entorno gráfico de gran usabilidad, donde se puede acceder a la funcionalidad de

todas las herramientas INTER-LAYER (a través de sus APIs, accesibles de manera unificada) y a funciones extra de control y monitorización de la solución aplicada en una capa.

INTER-FW es accesible como servicio web, integra seguridad por diseño y proporciona una REST API que unifica las APIs de todas las herramientas, a la que se puede acceder en modo REST o bien a través de la interfaz gráfica. También integra y soporta medidas de seguridad: las APIs de cada capa están protegidas con el uso de tokens de seguridad y uso de conexión segura con TLS.

Si bien las soluciones y herramientas de INTER-LAYER se pueden instalar y aplicar de manera independiente y aislada, este framework tiene el objetivo de hacer más cómodo y visual el uso y gestión de todas estas soluciones de interoperabilidad para el usuario, siendo una herramienta muy útil y completa.

5.3.3. Inter-Meth: metodología de implantación

Se creó una metodología específica, INTER-METH [192], que facilita y ofrece orientación sobre la implementación de INTER-IoT para integrar soluciones de interoperabilidad en sistemas y plataformas heterogéneas de IoT.

Además, se proporciona una herramienta gráfica, INTER-CASE, que guía la implementación de las soluciones de interoperabilidad de INTER-IoT, explicando la metodología para cada caso de implementación específico. Esta herramienta ofrece una evaluación paso a paso y una guía para este proceso.

La utilización de una metodología de ingeniería es de gran importancia en cualquier ámbito (por ejemplo, la ingeniería civil o la ingeniería de software) ya que maximiza y garantiza la eficacia de los procesos y las acciones a realizar. INTER-METH es el primer enfoque metodológico que permite la integración horizontal de plataformas de forma sistemática y manera integral. Esta metodología es de naturaleza iterativa y comprende seis etapas sucesivas: Análisis, Diseño, Implementación, Despliegue, Pruebas y Mantenimiento. En la práctica, y en función de las circunstancias particulares que se traten, es posible poner en bucle sólo determinadas etapas del proceso o bien conjuntos de etapas sucesivas, lo que facilita la adaptación a nuevos componentes y proporciona flexibilidad a esta técnica. Está fundamentada en el

diseño y uso de macropatrones de programación que representan una abstracción de los fundamentos en que se basan cada una las soluciones de interoperabilidad de INTER-IoT. En el marco de esta tesis doctoral se ha contribuido a la definición de los macropatrones de INTER-LAYER y a muchas tareas generales en el paquete de trabajo asociado para la definición de la metodología.

Esta metodología se complementó con un Libro de Recetas [193], o conjunto de tutoriales para el uso de las herramientas y las soluciones de interoperabilidad para casos básicos de uso.

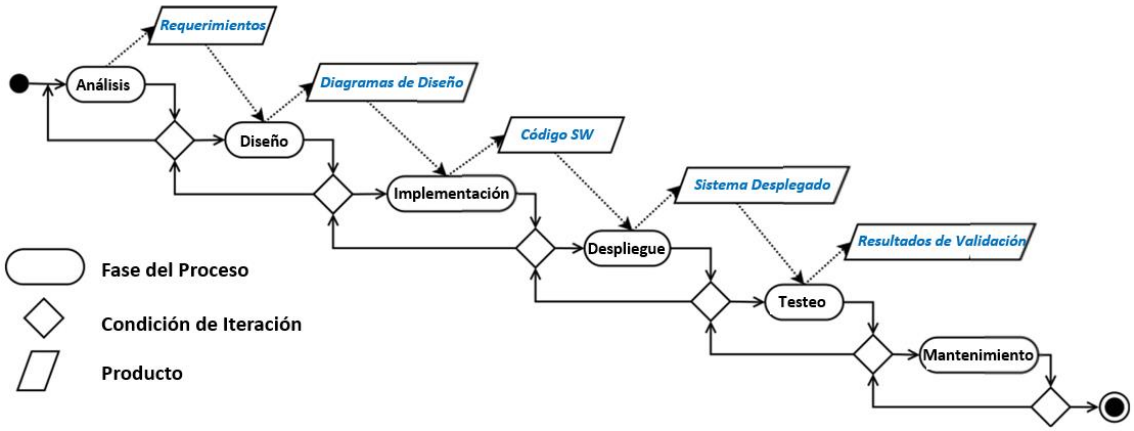


Figura 5.2. Procesos metodológicos de INTER-METH

5.4. Interoperabilidad Semántica Universal

Notablemente, entre el marco de herramientas para la interoperabilidad proporcionadas por INTER-IoT está el único traductor semántico para IoT existente hasta la fecha [35]. La técnica de traducción semántica en tiempo real entre dos modelos semánticos en IoT es completamente innovadora y novedosa, y tiene la capacidad de poder integrar horizontalmente a nivel de información plataformas IoT heterogéneas.

Esta solución de interoperabilidad puede proporcionar una traducción semántica automática entre cualquier par de plataformas [44]. La solución es un traductor semántico que realiza una traducción de ontología a ontología entre cualquier par de plataformas IoT, por lo que es capaz de proporcionar interoperabilidad semántica universal (DS2DS). En primer lugar, se puede considerar esta interoperabilidad universal ya que permite la traducción entre dos modelos semánticos de información cualquiera de manera general. En segundo lugar, esta interoperabilidad no se limita entre dos plataformas conectadas a través del IPSM, sino que es posible habilitar la interoperabilidad semántica entre un gran conjunto de plataformas, pudiendo cada una de ellas comunicarse e intercambiar información con cualquier otra del grupo mediante el uso de este traductor.

En esta sección se va a ver en detalle esta herramienta, y su potencial en el ecosistema IoT para disolver silos verticales y proporcionar interoperabilidad entre plataformas. Proporciona interoperabilidad a la información intercambiada entre plataformas gracias a su capacidad de adaptación y conversión de los modelos semánticos en que está representada esta información.

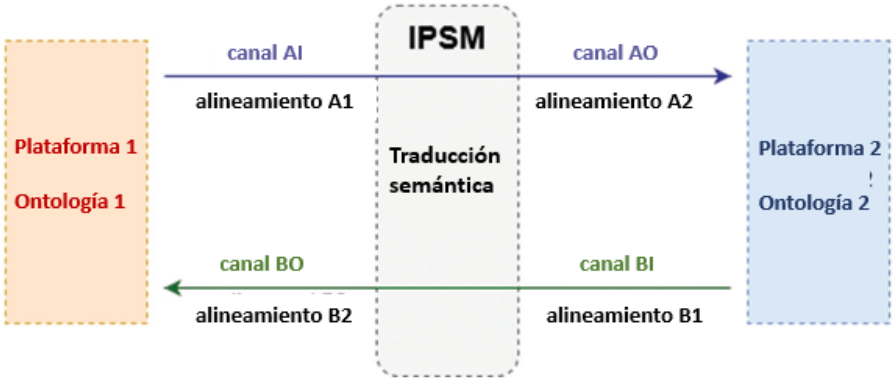


Figura 5.3 Traducción semántica inter-plataforma de ontología a ontología mediante el IPSM.

5.4.1. Elementos requeridos para la traducción

La solución de INTER-IoT para proporcionar interoperabilidad semántica entre plataformas IoT heterogéneas requiere los siguientes elementos:

- Una semántica explícita definida, delimitada por OWL, para cada plataforma IoT que deba interoperar, comunicarse y colaborar, y para ello requiera del uso de traducciones semánticas [34].
- Un traductor semántico que traduzca el flujo de mensajes y datos intercambiados entre dos plataformas, como un elemento intermedio entre ellas. Este traductor sería el IPSM y las plataformas, o elementos de comunicación con la plataforma, se conectarían al traductor a través de su API, a través de los denominados canales de entrada y salida. Requiere de configuración previa, y la carga anterior a la traducción de los alineamientos semánticos entre las ontologías de las plataformas y recibir la información en RDF.
- Una ontología modular central, en el caso de conectar más de dos plataformas o prever conectar más en el futuro. Una opción es la ontología para IoT desarrollada en el marco del proyecto INTER-IoT, denominada GOIoTP [79]. Hay que notar que el uso de una ontología central no es obligatorio pero es altamente conveniente.
- Los alineamientos semánticos entre ontologías o modelos semánticos de información entre las plataformas a interoperar.
- En el caso de que los mensajes y datos de las plataformas entrantes no estén en formato RDF (en concreto en la serialización JSON-LD) es necesario la utilización de un conversor sintáctico que adapte el formato de datos de entrada a JSON-LD.
- En el caso de que la plataforma de destino que recibe la información no soporte RDF, debe usarse un conversor sintáctico entre la salida del IPSM y la plataforma. Este conversor debe extraer el grafo de datos de los mensajes JSON-LD traducidos y convertirlo al formato de datos en que la plataforma espera recibir la información.

Las traducciones semánticas requieren de todo este conjunto de elementos de manera previa, para poder tener defini y garantizar la coherencia de formatos.

5.4.2. Estrategia de traducción de múltiples fuentes

El uso de una ontología central puede minimizar drásticamente el número de alineamientos distintos entre ontologías o modelo semánticos que hay que preparar cuando hay muchas plataformas a interoperar más de dos o tres plataformas a interoperar o se prevé la inclusión de plataformas futuras. Esta estrategia implica realizar una tradución intermedia a la hora de traducir semánticamente información de un modelo semántico A a otro B. De esta manera se realizaría una primera traducción de A a la ontología común, y una segunda de la ontología común a B. Esta estrategia implica que el número de alineamientos de una ontología a otra necesario para realizar traducciones entre un conjunto de plataforma (considerando e incluyendo cualquier combinación de ellas) se reduciría de manera multiplicativa mediante el uso de una ontología central en lugar de hacer traducciones directas entre todas ellas [7].

Esta estrategia de uso de una ontología central en las traducciones aporta gran escalabilidad en el caso de interconectar e incluir muchas fuentes, o para un futuro crecimiento del conjunto o ecosistema interoperable de plataformas.

5.4.3. Pasos para realizar una traducción semántica

Los pasos y requerimientos para poder realizar una traducción semántica entre varias entidades serían:

- Hacer un estudio semántico previo de los modelos de información y semántica de las entidades a comunicar (que podrían ser plataformas, aplicaciones u otro tipo de fuente o recepto de datos). Para ello hace falta tener definida la semántica de los artefactos a comunicar en RDF u OWL. En muchos casos en plataformas IoT se utilizan modelos de datos sin ningún tipo de relación, anotación o soporte semántico, y que no tienen definidas las relaciones y la estructura entre sus conceptos. En tal caso hace falta definir primero las relaciones y una descripción del modelo de datos en RDF o OWL, a partir del modelo de datos original. Este tipo de trabajo previo no es trivial y requiere de conocimientos semánticos.

- En el caso de tener los modelos semánticos en RDF y OWL y clarificado el significado y relación de sus conceptos o clases, se deben identificar y crear equivalencias y relaciones entre ambos, a fin de poder determinar alineamientos semánticos entre ellos.
- Crear alineamientos semánticos entre las dos ontologías o modelos de datos que traducir semánticamente. Se debe crear un fichero en RDF (bien en formato RDF/XML o Turtle) que contenga las reglas de traducción entre un modelo semántico y otro de forma unidireccional. Por tanto, para una comunicación bidireccional entre dos entidades serían necesarios varios alineamientos. Es necesario escribirlos utilizando el formalismo IPSM-AF [].
- -Instalar y configurar el IPSM con los alineamientos para realizar una traducción, y la fuente de entrada. En una misma instancia del IPSM es posible tener una gran cantidad de traducciones configuradas y entidades conectadas. Se definen canales (entradas y salidas al IPSM conectadas, entre las cuales se realiza una traducción semántica) en los que se debe indicar un alineamiento asociado para poder efectuar la traducción.
- Conectar las plataformas, y si es necesario, los adaptadores sintácticos. Los canales de comunicación funcionan en modo de publicación-suscripción, lo que permite que un solo canal sirva tanto para la comunicación uno a uno como para la comunicación uno a muchos.

5.4.4. Información gestionada por el IPSM

El IPSM traduce flujos de mensajes en tiempo real. Estos mensajes deben estar serializados en JSON-LD, soportando por tanto el uso de triples y anotaciones semánticas. Así mismo, también deben estar divididos en dos grafos de información:

- Un primer grafo donde se pueden almacenar metadatos, que es ignorado por el IPSM en el proceso de traducción
- Un segundo grafo que contiene la información IoT enviada por la plataforma o bien por otro tipo de fuente que haga uso del IPSM para realizar traducciones (ej. una aplicación).

5.4.5. Alineamientos

La creación de los ficheros almacenando la información de traducción entre modelos semánticos que necesita el IPSM para poder efectuarla requiere de un estudio previo de las alineaciones entre los dos modelos semánticos. Deben ser escritos utilizando el formalismo IPSM-AF. La primera parte del alineamiento son parámetros generales de traducción, como ontología fuente o destino o el tipo de sintaxis RDF que utiliza el alineamiento (Turtle o XML/RDF). La siguiente es un conjunto de celdas de traducción que ejecutan la traducción de conceptos semánticos en el orden en que se han generado.

Son unidireccionales en el sentido de que habilitan la traducción de manera unidireccional. Por tanto para habilitar traducciones en los dos sentidos (de la plataforma A a la B, y de la B a la A) es necesario crear dos, uno para cada sentido de traducción. En el caso de utilizarse una ontología central sería el mismo caso, pero teniendo en cuenta que hay una traducción intermedia por cada traducción de una plataforma A a otra B.

En el marco de esta tesis doctoral se han desarrollado múltiples alineamientos para la interoperabilidad semántica de la información entre plataformas concretas.

5.4.6. Configuración del IPSM

El IPSM debe ser previamente configurado para poder realizar las traducciones, definiendo:

- Los canales para la entrada y salida de datos de plataformas (u otras fuentes), de manera que la plataforma pueda enviar los datos.
- Que alineamiento está asociado a cada canal. Un canal podría no tener ninguno (y no hacer ninguna traducción) o tener dos (y hacer una traducción doble de manera secuencial).

La interfaz API del IPSM permite operaciones de gestión de alineamientos (creación o subida y eliminación) y de canales, así como uso del modo de traducción mensaje a mensaje en lugar de flujo de datos.

El IPSM puede tener un gran número de traducciones configuradas, siendo capaz también de efectuarlas simultáneamente.

5.4.7. GoIoTP: ontología para IoT

En el marco de este proyecto también se ha creado una ontología especialmente diseñada para el soporte genérico de información proveniente de sistemas IoT [73]. Está basada en W3C SSN/SOSA [75] y añade dos conceptos básicos principales: servicio y usuario. Por sus características, es muy adecuada como ontología central de traducción.

En el marco de esta tesis doctoral se contribuyó en tareas para la definición de un modelo de datos de INTER-IoT que representaría la primera aproximación para sentar las bases de la ontología GoIoTP [79] e investigar las necesidades de soporte de información de plataformas IoT.

5.4.8. Ecosistema interoperable de plataformas IoT

A nivel global, los beneficios más importantes que puede aportar el establecimiento de interoperabilidad semántica universal entre plataformas IoT heterogéneas es la posibilidad de integración horizontal de silos verticales, y de evitar la fragmentación del ecosistema global de IoT.

Sin embargo, la capacidad efectiva de integración horizontal de plataformas IoT heterogéneas utilizando esta solución, y con ellas el sistema IoT que gestiona y el conjunto de aplicaciones asociadas, depende de las capacidades y potencia de la solución particular actual. Es decir, que en el caso de tener grandes limitaciones de uso (como suele suceder con los prototipos) la interoperabilidad que se podría conseguir de manera global estaría también más limitada, aunque en cualquier caso se hubiesen abierto nuevas vías muy innovadoras que permiten la interoperabilidad semántica entre plataformas, y su desarrollo futuro podría permitir una aplicación de mayor alcance y efectividad.

En este sentido, esta solución permite crear ecosistemas interoperables de plataformas IoT dado que:

- Permite la interoperabilidad semántica entre cualquier par de plataformas IoT heterogéneas. Esto lo consigue al permitir la conversión (traducción semántica) del modelo semántico de la información entre dos modelos diferentes de manera general. No depende de que estas plataformas se hayan adherido a un estándar o a ciertas reglas, ni implica cambios invasivos en ellas. Tampoco que hayan seguido una ontología común (aunque alineaciones en los modelos de información facilitan una alta calidad de la traducción).
- Permite, además del paradigma de traducción uno a uno, creando un sistema interoperable de solo dos plataformas, la inclusión de más plataformas IoT en el conjunto en el sentido de que todas ellas puedan comunicarse e interoperar semánticamente con todas ellas. Esto permite la creación de un ecosistema interoperable de plataformas IoT, en el que se incluiría también a las aplicaciones y dispositivos asociados a ellas. En este sentido, sería necesario tener a las plataformas conectadas a un traductor o traductores, correctamente configurado, y haber definido los alineamientos de traducción necesarios.
- Permite añadir (o quitar) plataformas IoT en este ecosistema en cualquier momento. Es decir, que el conjunto de plataformas no sería fijo y dependería de las incluidas inicialmente. Esto aporta flexibilidad al ecosistema, y lo hace viable para su crecimiento y evolución. Si fuera fijo inicialmente, esta integración de plataformas e interoperabilidad semántica estaría muy limitada respecto al conjunto de plataformas de aplicación y completamente restringido respecto a su crecimiento y evolución.
- Mediante la estrategia del uso de una ontología central permite que un ecosistema interoperable de plataformas sea escalable, característica que es crítica para el crecimiento potencial de este ecosistema. Si cada plataforma que se incluye en el ecosistema tuviera que crear 2 alineamientos para comunicarse con cada plataforma ya integrada en él, a medida que el ecosistema creciera y tuviera más miembros, la inclusión de una nueva se volvería exponencialmente más costosa. Este factor acabaría limitando el número de plataformas y futuro crecimiento, que tendería a ser reducido. El uso de una ontología central es una estrategia que permite que el esfuerzo de inclusión de una plataforma se limite a la creación de dos alineamientos para

poder comunicarse con todas las demás, siendo por tanto el esfuerzo de inclusión lineal (incluso aunque fuese conveniente algún ajuste en algún otro alineamiento). Esta estrategia permite un esfuerzo de crecimiento lineal, siendo el coste de inclusión de una nueva plataforma similar al coste de inclusión de las plataformas anteriores, o las que estaban inicialmente en él. La estrategia de uso de una ontología central aporta dos características clave al ecosistema interoperable: capacidad de crecimiento (con esfuerzo lineal respecto al número de plataformas) así como escalabilidad.

- La información IoT en los sistemas y plataformas fluye en flujos de datos masivos a gran velocidad (IoT Big Data), lo que implica que una estrategia de interoperabilidad mediante traducciones semánticas debe ser capaz de gestionar y traducir grandes volúmenes de datos a gran velocidad, en tiempo real o casi real. En este sentido el IPSM es una herramienta capaz de este tipo de gestión.
- En una línea parecida, el IPSM es una herramienta capaz de gestionar, no solo un canal de traducción entre dos plataformas, traduciendo el flujo de datos e información entre ellas en tiempo real, sino que también es capaz de efectuar las traducciones en un gran número de canales de traducción entre plataformas simultáneamente sin pérdida de rendimiento. En ese sentido, es una herramienta con buena escalabilidad.
- Un ecosistema interoperable, además, podría utilizar distintos IPSM realizando las traducciones de manera distribuida, o permitiría la conexión y unión (parcial o total) con otros ecosistemas interoperables que utilizan este tipo de solución.

Se puede concluir que es una solución bien diseñada para soportar el establecimiento, crecimiento y evolución de ecosistemas interoperables de plataformas IoT, y es capaz de proporcionar “interoperabilidad semántica universal”, entendiendo por ello a la capacidad de establecer interoperabilidad semántica entre cualquier par de plataformas IoT heterogéneas.

También se puede concluir que las características vistas de esta solución permiten la integración horizontal de silos verticales, y puede facilitar en gran medida la evolución de la situación fragmentada actual del ecosistema global de IoT a un ecosistema global

sin barreras de interoperabilidad. Esto permitiría un gran flujo de información entre los distintos sistemas y plataformas, así como sus conjuntos de aplicaciones nativas, sin la barrera de la interoperabilidad, permitiendo la explotación a gran escala de la información IoT, compatir información valiosa entre ellas, sinergias muy importantes entre dominios o actores clave en un dominio, así como aplicaciones interoperables y flujo entre ellas.

Es importante notar, en este sentido, que esta interoperabilidad entre plataformas también tiene implicación en la capa de aplicaciones asociadas a una determinada plataforma (entendida como instancia concreta de la plataforma). Las aplicaciones que utilizan información IoT son específicas para los formatos y modelos de información de la plataforma de la que obtienen esta información, y obtienen los datos interactuando con las interfaces y protocolos para obtener información de esta plataforma. Por ello, son "nativas" a una instancia de plataforma.y no pueden funcionar con otras. También, por la misma razón, no pueden generalmente gestionar múltiples fuentes si provienen de distintas plataformas, habiendo barreras de interoperabilidad que dificultan esta posibilidad. La aplicación de esta solución semántica de interoperabilidad permite disolver estas barreras de interoperabilidad, permitiendo que una aplicación pueda recibir información de múltiples plataformas con el modelo semántico de la información de la plataforma que es nativa, por ejemplo.

5.5. Validación de las soluciones de interoperabilidad para distintos casos de uso y dominios de aplicación

Las soluciones de interoperabilidad se aplicaron en distintos dominios en los que había necesidades de interoperabilidad.

En primer lugar, se aplicaron en los dos pilotos del proyecto (Inter-Health [39] e Inter-LogP [188]) en las áreas de salud y de transporte y logística portuaria respectivamente.

En ambos casos se integraron horizontalmente distintas plataformas con un papel diferente dentro de un dominio concreto (salud o transporte y logística). Esta

integración se realizó mediante el uso de las soluciones de interoperabilidad a nivel de plataforma, y se validaron distintas herramientas y soluciones de INTER-IoT. Fruto de la interoperabilidad habilitada, se permitió el intercambio de información y la colaboración entre distintas plataformas IoT, que gestionaban distintos datos. Esto generó sinergias entre ellas y permitió crear un servicio de monitorización de salud remoto, utilizando wearables en el caso de Inter-Health, y la realización de distintas funciones automáticas y servicios innovadores para la gestión portuaria en Inter-LogP que no habrían sido posibles sin la colaboración de distintas plataformas IoT de gestión portuaria en distintas áreas y pertenecientes a distintas entidades.

Otros casos de aplicación y validación de las soluciones de IoT, utilizando estas herramientas en muy distintos dominios desde Prevención de Plagas a Ciudades Inteligentes se realizó por socios externos que colaboraron con el proyecto INTER-IoT a través de una convocatoria abierta financiada por la Comisión Europea. Las soluciones de INTER-IoT se aplicaron en los distintos dominios propuestos, formando parte de una solución IoT determinada en ese dominio, o inclusive, las distintas herramientas y componentes fueron extendidos.

Actualmente las soluciones se han adoptado en otros proyectos H2020 como PIXEL [194] (Inter-MW) para gestión medioambiental portuaria, H2020 5GENESIS [195][196] (pasarela de red INTER-IoT para el uso de redes 5G y SDN) y LSP H2020 ACTIVAGE [197] en el ámbito de Envejecimiento Activo y Saludable (AHA), validando su uso en todas ellas.

Debido a su capacidad innovadora para proporcionar interoperabilidad completa entre plataformas IoT heterogéneas, que no siguen estándares comunes que permiten su interoperación, se espera su adopción futura por desarrolladores, empresas y entidades de investigación para proyectos en los que sea necesaria la interoperabilidad en IoT – en especial a nivel de plataforma a nivel semántico, creándose más ejemplos de su aplicación y validación en distintos dominios de IoT. Estas soluciones se pueden aplicar en cualquier dominio o a través de múltiples dominios donde haya una necesidad de interoperabilidad.

De entre todos estos casos de uso validando la interoperabilidad entre plataformas heterogéneas conseguida a través de las soluciones de INTER-IoT, en esta sección se

ve en detalle la validación de la interoperabilidad semántica en el piloto de salud Inter-Health.

5.5.1. Validación de la interoperabilidad semántica entre plataformas heterogéneas: Inter-Health

Uno de los pilotos del proyecto INTER-IoT consistió en la creación de un sistema de sistemas IoT en el área de la salud para proporcionar un servicio de monitorización, control y prevención de la obesidad y fomento de hábitos de vida saludables. Este servicio es una optimización por medio de la tecnología IoT del proceso de seguimiento clásico de la evolución de sujetos adheridos a un programa médico, y ofrece una monitorización continua en el tiempo de indicadores de salud bajo la observación profesional en todo momento, de manera remota desde el domicilio del paciente, sin necesidad de desplazarse al centro de salud. Inclusive, también permite la monitorización móvil de indicadores de actividad física mientras se hace deporte fuera de un recinto mediante el uso de sensores IoT corporales y una plataforma y pasarela IoT portable.

Este sistema de sistemas requirió de la integración horizontal de varias plataformas IoT heterogéneas (inicialmente universAAL y BodyCloud) mediante el uso de las soluciones para la interoperabilidad semántica de INTER-IoT. Además, se realizó una extensión para poder recoger medidas de seguimiento de indicadores de salud adquiridas por dispositivos IoT de Hogares Inteligentes, los cuales estaban gestionados por otras plataformas (SOFIA2 y FIWARE).

Mediante la integración de varias plataformas IoT el objetivo fue crear una plataforma sanitaria más potente para la monitorización del estilo de vida de individuos, que pudiera implementar nuevas aplicaciones y servicios que las plataformas individuales no podrían soportar. El enfoque interoperable propuesto permite el desarrollo de nuevos servicios multiplataforma sobre ellas.

En el programa médico para fomentar un estilo de vida saludable y prevenir la obesidad y las enfermedades crónicas derivadas se realizan sesiones de asesoría nutricional y hábitos saludables y se aplica un seguimiento de indicadores de salud de los usuarios finales (características físicas, comportamiento nutricional y la actividad

física). Existen diversos indicadores que medir y analizar para prevenir y detectar la obesidad siguiendo el protocolo médico dado por la Organización Mundial de la Salud (OMS) [198]. A través de estos indicadores es posible determinar el estado de salud en términos de peso adecuado o inadecuado (los niveles varían desde el bajo peso, el peso normal, el sobrepeso hasta la obesidad). El seguimiento de estos indicadores se realiza generalmente de manera tradicional y requiere de la visita al centro de salud para actualizarlo. Sin embargo, una monitorización a distancia utilizando la tecnología IoT podría permitir un seguimiento más eficaz y con una actualización muy frecuente, con la observación y supervisión en todo momento de profesionales. Este seguimiento ayudaría a una mayor eficacia del programa, ya que, por ejemplo, los médicos y nutricionistas pueden realizar un seguimiento continuo día a día y acciones de supervisión y ajuste inmediatas en el caso de considerarlo necesario.

En el piloto INTER-Health [39] [198] se crea un entorno de Vida Cotidiana Asistida (AAL) que permite la medición remota de diferentes parámetros fisiológicos por medio de dispositivos médicos IoT, como una báscula, un tensiómetro y sensores de actividad física [199]. Los dispositivos IoT mencionados interactúan con una plataforma IoT (BodyCloud o UniversAAL), y proporcionan mediciones a través de la conexión mediante tecnología Bluetooth con una pasarela inteligente [142]. Esta pasarela inteligente de red recibe las medidas de los dispositivos y las envía a la plataforma IoT a través de la conectividad disponible (ej. 2G/3G/4G/Wi-Fi/ADSL). Desde la plataforma, esta información se envía a una aplicación médica para el seguimiento de los pacientes, a la que tienen acceso los médicos y nutricionistas del programa, además de sus usuarios, que pueden observar en ella su evolución. Esta aplicación recibe y puede utilizar datos de las dos plataformas gracias al uso de soluciones de interoperabilidad de INTER-LAYER (Inter-MW).

El sistema completo y la integración de plataformas IoT heterogéneas dentro de él puede verse en la Figura 5.4.

En el marco de esta tesis doctoral se contribuyó en la realización de una extensión para poder incluir información de dispositivos IoT de otras plataformas (SOFIA2 y FIWARE) utilizadas en Hogares Inteligentes ya establecidos. La integración de los datos de medidas de indicadores desde estas plataformas en lugar de hacerse directamente en la aplicación se decidió realizarse a través de la plataforma

universAAL ya que realizaba el control de usuarios general en el centro de salud y esto ofrecía ciertas ventajas. La interconexión entre las plataformas SOFIA2 o FIWARE y universAAL se realizó empleando la solución para la habilitación de interoperabilidad semántica de INTER-LAYER.

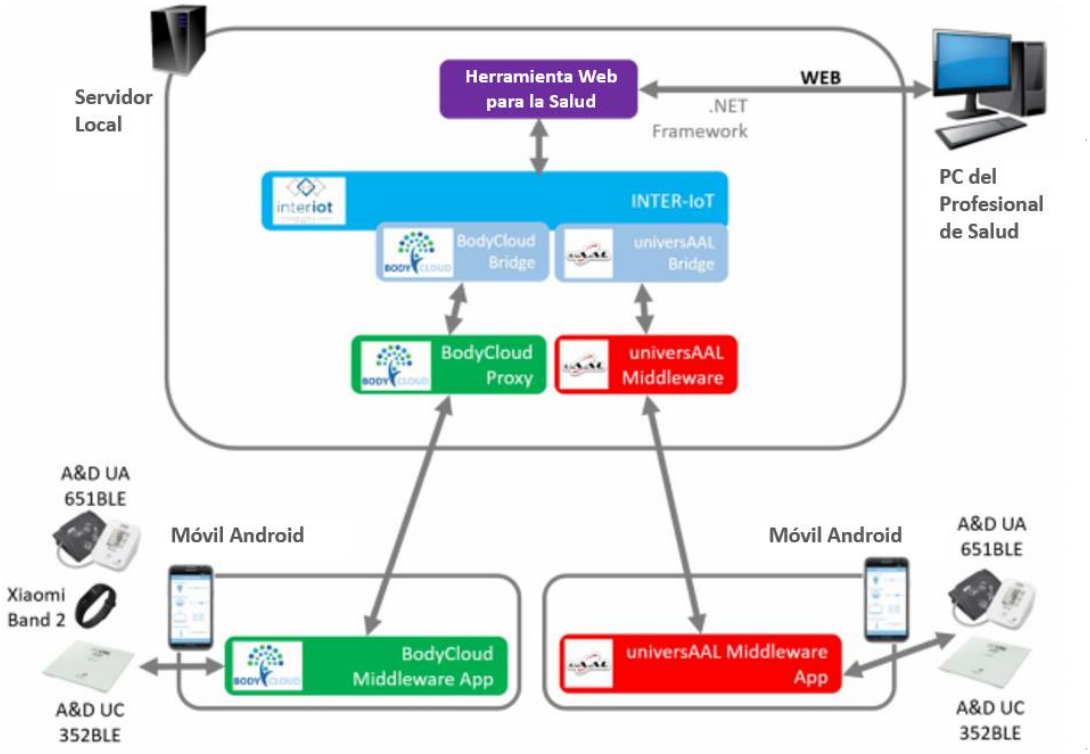


Figura 5.4 Visión general del sistema sanitario de INTER-Health.

A través de la aplicación médica web, los médicos pueden realizar un seguimiento de los pacientes a distancia en cualquier momento, ponerse en contacto con ellos a través de las herramientas de comunicación TIC (SMS, correo electrónico, teléfono y teleconferencia) y darles una valoración médica.

Este programa para la adquisición de hábitos saludables para el control de la obesidad y enfermedades crónicas derivadas se realizó en un Centro Nacional de Salud italiano

utilizando a la vez en un grupo de prueba que utilizó métodos tradicionales de seguimiento, y el sistema piloto INTER-Health para la monitorización continua y a distancia de indicadores utilizando la tecnología IoT en otro grupo de prueba de características. Ambos grupos de estudio estaban compuestos por 100 personas cada uno.

Junto con una primera sesión de asesoramiento nutricional en el centro médico, se realiza también una primera medida de indicadores de salud de cada individuo (Índice de Masa Corporal, circunferencia de la cintura, peso, presión arterial y otros). Los sujetos deben visitar el centro médico y nutricional cada 6 meses para realizar revisiones. El grupo que utiliza la solución tecnológica de INTER-Health tiene acceso a una aplicación web del programa de salud desde la que puede ver su seguimiento e interactuar con ella. En ella se registra la evolución de sus indicadores de salud recogidos por dispositivos IoT desde sus casas. El profesional sanitario encargado del seguimiento de cada usuario tiene acceso al historial de todas las mediciones a través de esta aplicación y puede interactuar con el paciente si lo considera conveniente. El grupo que emplea el sistema tradicional simplemente cumplimenta fichas entre visita y visita al centro médico. Al finalizar el programa se compararon los avances entre el grupo que utilizaba el sistema IoT de seguimiento y el grupo que solo empleaba métodos de monitorización tradicional, comprobando las ventajas de la utilización de la tecnología IoT en el seguimiento médico de pacientes y validando la solución para la interoperabilidad semántica de INTER-IoT.

5.5.1.1 *Funcionalidades técnicas de INTER-Health*

El sistema IoT resultante de la integración de las distinas plataformas tiene las siguientes funcionalidades principales:

- Recogida de medidas objetivas (peso, talla, índice de masa corporal, presión arterial o perímetro de la cintura) y subjetivas (cuestionarios sobre los hábitos alimentarios y la práctica de actividad física) durante las visitas al centro de salud. Estas medidas están realizadas en la plataforma universAAL.
- Telemonitorización en el centro sanitario de las medidas subjetivas (cuestionarios) y objetivas (peso, presión arterial, etc...) enviadas por los

pacientes en su domicilio (basado en la plataforma UniversAAL y extendido a las plataformas FIWARE y SOFIA2);

- Telemonitorización en el centro sanitario de las actividades físicas realizadas por el paciente con dispositivos wearables (recogidos desde la plataforma BodyCloud), a la que podían añadirse otras medidas con dispositivos IoT de salud. La plataforma BodyCloud instalada en un teléfono móvil lo convierte en una pasarela IoT portable a la que pueden conectarse sensores. Esto permite el uso de sensores portables o wereables para la monitorización de la actividad física, creándose una red corporal de sensores (BSN o Body Sensor Network) en la persona en observación.

Esto permite acceder desde la aplicación al informe y visualización de todas las mediciones recogidas para su análisis e interacción en los tratamientos.

5.5.1.2 *Extensión para la medida y monitorización con otras plataformas*

Distintos usuarios ya tenían incorporados sensores IoT en Hogares Inteligentes que proporcionaban monitorización del peso y otros indicadores de salud. Dado que el peso es la medida más importante bajo observación, siendo las otras deseables pero menos significativas, se optó por incluir estos usuarios y mediciones mediante una solución de interoperabilidad entre plataformas, extendiendo el sistema-de-sistemas para que pudiera recoger también las medidas provenientes de plataformas FIWARE y SOFIA2. Se integraron las medidas de peso y de tasa de latidos.

Hay que tener en cuenta que tanto FIWARE como SOFIA2 son plataformas IoT no propietarias muy utilizadas para la gestión IoT de Hogares Inteligentes (FIWARE a nivel europeo y SOFIA2 a nivel nacional en España), y que las básculas inteligentes son un dispositivo IoT muy frecuentemente utilizado (actualmente son más comunes que las básculas clásicas). Por estas razones se consideró interesante realizar una extensión del sistema para poder ser usado, no solo desde una plataforma universAAL, sino también desde plataformas FIWARE o SOFIA2 ya existentes que gestionasen las medidas de una báscula desde Hogares Inteligentes. De esta manera se podría incluir inmediatamente usuarios sin que tuvieran que preparar toda la instalación IoT y configuración previa en su casa (pasarela inteligente conectada a universAAL, báscula

compatible, APP de universAAL, plataforma IoT universAAL en un servidor, configuración y gestión de la plataforma, etc..). De esta manera, se ahorran muchos costes de tiempo, recursos y esfuerzo de instalación, y se permite añadir a estos usuarios de manera fácil e inmediata, y beneficiarse del servicio de control y prevención de la obesidad de INTER-Health. Mediante el uso de la tecnología también es posible sustituir las visitas físicas al centro de salud en Italia por videoconferencias en las que se guía de manera personal al sujeto adherido al programa de hábitos saludables.

Se optó por realizar la gestión de estas medidas desde la plataforma universAAL, ya preparada y habilitada para la gestión de usuarios y medidas de peso en domicilio y sobre la cual se emplea la Aplicación Web de Monitorización a la que pueden acceder personas en observación y médicos. Fue necesario añadir nuevos usuarios y dispositivos virtuales en esta plataforma para incluir a los provenientes de las plataformas FIWARE y SOFIA2, lo que resulta una operación muy sencilla y rápida de realizar. Por otro lado, se envió la información de sensores desde las plataformas externas a la plataforma universAAL utilizando el IPSM como elemento intermedio, el cual convertía el modelo semántico de representación de la información de la medida de peso, báscula y hogar de las plataformas FIWARE y SOFIA2 a su representación equivalente en universAAL. Para ello fue necesario desarrollar un alineamiento de traducción en cada caso.

Fue necesario hacer uso de una instancia del IPSM a la que se conectaba el flujo de información de la plataforma o plataformas de FIWARE, mientras que su salida se y su salida a la plataforma universAAL que gestionaba distintos usuarios y medidas para el control de indicadores de salud en el sistema INTER-Health. Previamente hubo que desarrollar un alineamiento semántico entre el modelo de datos de FIWARE y la ontología de universAAL y que configurar esta traducción en el IPSM. Estas mismas operaciones fueron necesarias para la integración de la plataforma o plataformas de SOFIA2, utilizando la misma instancia del IPSM con una diferente configuración de traducción y un alineamiento semántico distinto, específicamente diseñado habilitar la traducción entre ambos modelos semánticos de información.

En ambos casos el alineamiento a desarrollar tenía la complejidad de cambiar la representación de la información de un modelo sencillo conteniendo duplos de

campo y valor (o campo tipo y valor) a un modelo semánticamente más complejo capaz de soportar anotaciones semánticas y triples como es el caso de universAAL. Por esta razón, el alineamiento de traducción realizado en el sentido de SOFIA2 o FIWARE a universAAL es significantemente más complejo que esta misma alineación en el sentido inverso.

En las siguientes secciones pueden verse detalles de los intercambios de información entre las plataformas mediante la habilitación de interoperabilidad semántica con la solución de INTER-IoT para la capa de datos y semántica (uso del IPSM y alineamientos de traducción).

Extensión del sistema para plataformas IoT SOFIA2

Las plataformas SOFIA2 para el control de indicadores vitales de salud de manera remota, desde el domicilio, son utilizadas a nivel nacional. El modelo de datos es el genérico utilizado por la empresa Televés para proporcionar este tipo de servicio a través de SOFIA2, y está ampliamente utilizado por un gran conjunto de usuarios en España.

Se pueden notar las diferencias entre los dos modelos sintácticos y semánticos de representación de la información utilizados en cada una de las plataformas en las Tabla 4.1, 4.2 y 4.3. La Tabla 4.1 representa la información recogida por la báscula desde SOFIA2, mientras que la Tabla 4.2 muestra la representación de esa misma información en la plataforma universAAL, utilizando su ontología propia sin extensiones. Un análisis campo a campo se puede ver en la Tabla 4.3. Cada campo representa un concepto clave. Algunos campos de información que se pueden ver en los mensajes no están incluidos en algunos casos por ser información propia de la plataforma (“Origen” hace referencia al enrutador o pasarela conectado a SOFIA2, y no tiene sentido en universAAL ni guarda ninguna información relevante desde el punto de vista de control de obesidad). También hay que notar que en el mensaje en universAAL están recogidas relaciones entre datos y conceptos semánticos lo que hace el mensaje significantemente más extenso. En cualquier caso, a pesar de la diferencias diferencias de extensión y representación de los mensajes los datos clave

que recogen la información proporcionada por la báscula están presentes en ambos, bajo una representación distinta.

Fue necesario crear un alineamiento semántico para la traducción de la información desde la ontología o modelo de datos de SOFIA2 a la ontología destino de universAAL, analizando previamente las relaciones entre los distintos modelos de representación de la información. La traducción fue configurada en el IPSM almacenando la información del alineamiento y configurando la traducción semántica. En este caso solo se realiza la traducción de una medida, pero podrían añadirse fácilmente otras similares.

Por un lado universAAL utiliza la sintaxis Turtle (una serialización de RDF) y es capaz de soportar anotaciones semánticas y relaciones semánticas entre el conjunto de datos contenidos, mientras que SOFIA2 utiliza la sintaxis JSON que solo permite el uso de un conjunto de campos y su valor asociado. En cualquier caso, la información en el formato de cada una de las plataformas se preserva a través de la traducción semántica.

Se puede notar que hacen falta conversiones de tipo de unidad temporal a la hora de notar el momento en que se produjo la medida del peso, ya que mientras SOFIA2 utiliza el formato de fecha y hora, universAAL sigue el formato timestamp (segundos desde 1/1/1970).

También se puede observar que los formatos de las unidades están representados de manera muy diferente y que en universAAL se emplea la composición de un prefijo y unidad base mientras que SOFIA2 utiliza una unidad completa predefinida. Como la unidad en sí es la misma no es necesaria ninguna operación de conversión de unidad, pero este tipo de diferencias o detalles particulares en el modo de representación han estar considerados en el mapeo de traducción.

Otro detalle significativo que se puede observar en la tabla de equivalencia o alineamiento de conceptos semánticos es la distinta resolución en las medidas entre

ambas plataformas. Esto implica la añadidura de mayor precisión en la medida final mediante una conversión.

Los identificadores de dispositivo son diferentes en cada plataforma, ya que cada una los referencia de manera diferente. El identificador de SOFIA2 hace referencia al sensor real, el identificador de universAAL al sensor virtual dentro de esta plataforma que resulta un "sensor espejo" del real. Este cambio no se realiza a través de la traducción semántica ya que no es una diferencia de significado o representación, sino una asignación de intercambio. El cambio se hace a nivel de middleware a través del uso de una tabla de equivalencia de identificadores, y se podría realizar de otras maneras de forma sencilla (por ejemplo utilizando Inter-MW o una función o servicio que cambie las asignaciones de intercambio). Esto sería así solamente para los identificadores de dispositivo y podría darse el caso también con el concepto de usuario asociado. No es necesario hacer un cambio de identificador de paciente ya que en universAAL están asociados internamente a los dispositivos ya registrados.

Tabla 5.1 Medidas de tomadas desde la plataforma SOFIA2 y representadas de acuerdo a su modelo de datos.

{
"Biomedida": {
"origen":"00110011001100",
.."idDispositivo":"E8-EB-11-0B-19-30",
.."idPaciente":"2105652",
"idProfesional":"ABC45676",
"valor":"50",
"tipo":"PESO",
.."unidad":"ppm",
"fechaActividad":"2021-03-21T10:41:00.263Z"
}
}
	{
	"Biomedida": {
	"origen":"00110011001100",
	.."idDispositivo":"E9-8A-11-DE-92-10",
	.."idPaciente":"2105652",
	"idProfesional":"ABC45676",
	"valor":"83",
	"tipo":"PPM",
	.."unidad":"ppm",
	"fechaActividad":"2021-03-21T10:45:00.344Z"
	}
	}

Tabla 5.2 Medidas de la báscula y el pulsómetro de SOFIA2 traducidas a la representación semántica de la información de la ontología de universAAL

@prefix ns: <http://ontology.universAAL.org/InterIoT.owl#> . @prefix ns1: <http://ontology.universaal.org/PhThing.owl#> . @prefix ns2: <http://ontology.universaal.org/Measurement.owl#> . @prefix xsd: <http://www.w3.org/2001/XMLSchema#> . @prefix ns3: <http://ontology.universaal.org/HealthMeasurement.owl#> . @prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> . @prefix ns4: <http://ontology.universAAL.org/Device.owl#> . @prefix : <http://ontology.universAAL.org/Context.owl#> . <urn:org.universAAL.middleware.context.rdf:ContextEvent#_:7f000101a5f8b64a:453>:hasProvider <http://ontology.universAAL.org/WeightingDeviceContextPublisher> ; a :ContextEvent ; rdf:subject ns1:scale; :hasTimestamp "1616323260263"^^xsd:long ; rdf:predicate ns4:hasValue ; rdf:object ns1:weight. :gauge a :ContextProviderType . http://ontology.universAAL.org/WeightingDeviceContextPublisher> a :ContextProvider ; :hasType :gauge . :myClassesOfEvents [a :ContextEventPattern; <http://www.w3.org/2000/01/rdf-schema#subClassOf> [a owl:Restriction; owl:allValuesFrom ns5:WeighingScale; owl:onProperty rdf:subject]]. ns1:weight a ns3:PersonWeight, ns2:Measurement , ns3:HealthMeasurement ; ns2: hasUnit <http:ontology.universAAL.org/Unit.owl#gram> ns2: hasPrefix <http:ontology.universAAL.org/Unit.owl#kilo> ns2:value "50.0"^^xsd:float .	@prefix ns: <http://ontology.universAAL.org/InterIoT.owl#> . @prefix ns1: <http://ontology.universaal.org/PhThing.owl#> . @prefix ns2: <http://ontology.universaal.org/Measurement.owl#> . @prefix xsd: <http://www.w3.org/2001/XMLSchema#> . @prefix ns3: <http://ontology.universaal.org/HealthMeasurement.owl#> . @prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> . @prefix ns4: <http://ontology.universAAL.org/Device.owl#> . @prefix : <http://ontology.universAAL.org/Context.owl#> . <urn:org.universAAL.middleware.context.rdf:ContextEvent#_:7f000101a5f8a64a:f83>:hasProvider <http://ontology.universAAL.org/ForaBloodpressureContextPublisher> ; a :ContextEvent ; rdf:subject <http://ontology.universAAL.org/InterIoT.owl#b8:27:eb:44:d6:d9BP> ; :hasTimestamp "1616323500344"^^xsd:long ; rdf:predicate ns4:hasValue ; rdf:object _:BN000000 . :gauge a :ContextProviderType . <http://ontology.universAAL.org/ForaBloodpressureContextPublisher> a :ContextProvider ; :hasType :gauge . _:BN000000 a ns3:HeartRate , ns2:Measurement , ns3:HealthMeasurement ; ns2:value "83"^^xsd:int . <http://ontology.universAAL.org/InterIoT.owl#b8:27:eb:44:d6:d9BP> a <http://ontology.universAAL.org/PersonalHealthDevice.owl#HeartRateSensor> , ns1:Device , ns1:PhysicalThing ; ns4:hasValue _:BN000000 .

Tabla 5.3 Esquema de traducción de conceptos semánticos clave entre la información compartida por la fuente (SOFIA2) utilizando su propio modelo de información y su representación al enviarse a la plataforma destino universAAL, utilizando su ontología propia como soporte.

	Modelo de datos de SOFIA2 (ontología origen)		**Ontología genérica de universAAL (ontología destino)**	
	Campo	***Valor (muestra)***	***Campo***	***Valor (muestra)***
ID de dispositivo	idDispositivo	E8-EB-11-08-19-30	http://www.w3.org/1999/02/22-rdf-syntax-ns#subject	http://ontology.universAAL.org/InterIoT.owl#WeighingScale
Tiempo de medida	fechaActividad	2018-07-21T10:47:00.000Z	http://ontology.universAAL.org/Context.owl#hasTimestamp	1418143893015
Magnitud medida	tipo	PESO	http://ontology.universaal.org/Measurement.owl#type	ns1:http://ontology.universAAL.org/InterIoT.owl#weight
Valor	valor	50	http://ontology.universaal.org/Measurement.owl#value	50.0
Unidad	unidad	kg	ns2:hasPrefix ns2:hasUnit	http://ontology.universAAL.org/Unit.owl#kilo http://ontology.universAAL.org/Unit.owl#gram

Estas relaciones son similares al otro intercambio de información IoT habilitado, la medida de pulsaciones, como puede verse en la Tabla 4.2. Esta extensión sería ampliable a la hora de incluir otros tipos de sensores mediante una actualización del alineamiento.

Extensión del sistema para plataformas IoT FIWARE

De manera similar, se realizó la misma extensión en Inter-Health para integrar medidas y usuarios provenientes de plataformas FIWARE. Aunque FIWARE tiene un modelo de datos flexible y permite representar la información de múltiples maneras, se tomó como referencia para modelar mensajes de información el modelo de datos recomendado por la organización FIWARE para definir este tipo de medidas,

utilizando el estándar NGSI v2 [200][201]. Los Hogares Inteligentes gestionados por una plataforma FIWARE emplearán con mayor probabilidad este tipo de representación.

El formato de mensajes de FIWARE guarda importantes similitudes con SOFIA2: ambos utilizan una sintaxis de campo y valor asociado y no proporcionan soporte para anotaciones semánticas. También se puede ver un paralelismo relativo entre los distintos campos, que no llega a ser exacto pero sí bastante parecido. Mientras que en SOFIA2 directamente se asignaba un valor *string* a los campos, en este modelo de datos de FIWARE se asocia a cada campo un duplo conteniendo el tipo de datos representado y el valor del campo original respectivamente.

Tabla 5.4 Medida de la báscula (izquierda) y el pulsómetro (derecha) recogidas desde la plataforma FIWARE y representadas con su modelo con el formato de datos de FIWARE


```
{  "id": "device:FIW:LD:test001",
   "type": "Balance",
   "observation": {
      "type": "Number",
      "value": "73",
      "metadata": {
         "timestamp": {
            "value": "2017-06-17T07:21:24.238Z",
            "type": "DateTime"
         },
         "observationId": {
            "type": "String",
            "value": "scale-3343-001a"
         },
         "quantityKind": {
            "type": "String",
            "value": "weight"
         },
         "measurementUnit": {
            "type": "String",
            "value": "kilogram"
      }}}}
```

```
{  "id": "device:FIW:MD:test001",
   "type": "HeartBeatSensor",
   "observation": {
      "type": "Number",
      "value": "95",
      "metadata": {
         "timestamp": {
            "value": "2017-06-17T07:28:55.271Z",
            "type": "DateTime"
         },
         "observationId": {
            "type": "String",
            "value": "heartbeatsensor-030-001b"
         },
         "quantityKind": {
            "type": "String",
            "value": "heartbeat"
         },
         "measurementUnit": {
            "type": "String",
            "value": "bpm"
      }}}}
```

Tabla 5.5 Medidas de la báscula y el pulsómetro de FIWARE traducidas a la representación semántica de la información de la ontología de universAAL

@prefix ns: <http://ontology.universAAL.org/InterIoT.owl#> . @prefix ns1: <http://ontology.universaal.org/PhThing.owl#> . @prefix ns2: <http://ontology.universaal.org/Measurement.owl#> . @prefix xsd: <http://www.w3.org/2001/XMLSchema#> . @prefix ns3: <http://ontology.universaal.org/HealthMeasurement.owl#> . @prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> . @prefix ns4: <http://ontology.universAAL.org/Device.owl#> . @prefix : <http://ontology.universAAL.org/Context.owl#> . <urn:org.universAAL.middleware.context.rdf:ContextEvent#_:7f000101a5f8b64a:453>:hasProvider <http://ontology.universAAL.org/WeightingDeviceContextPublisher> ; a :ContextEvent ; rdf:subject ns1:scale; :hasTimestamp "1497694884238"^^xsd:long ; rdf:predicate ns4:hasValue ; rdf:object ns1:weight. :gauge a :ContextProviderType . http://ontology.universAAL.org/WeightingDeviceContextPublisher> a :ContextProvider ; :hasType :gauge . :myClassesOfEvents [a :ContextEventPattern; <http://www.w3.org/2000/01/rdf-schema#subClassOf> [a owl:Restriction; owl:allValuesFrom ns5:FIW33; owl:onProperty rdf:subject]]. ns1:weight a ns3:PersonWeight, ns2:Measurement , ns3:HealthMeasurement ; ns2: hasUnit <http:ontology.universAAL.org/Unit.owl#gram> ns2: hasPrefix <http:ontology.universAAL.org/Unit.owl#kilo> ns2:value "73.0"^^xsd:float .	@prefix ns: <http://ontology.universAAL.org/InterIoT.owl#> . @prefix ns1: <http://ontology.universaal.org/PhThing.owl#> . @prefix ns2: <http://ontology.universaal.org/Measurement.owl#> . @prefix xsd: <http://www.w3.org/2001/XMLSchema#> . @prefix ns3: <http://ontology.universaal.org/HealthMeasurement.owl#> . @prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> . @prefix ns4: <http://ontology.universAAL.org/Device.owl#> . @prefix : <http://ontology.universAAL.org/Context.owl#> . <urn:org.universAAL.middleware.context.rdf:ContextEvent#_:7f000101a5f8a68c:34b>:hasProvider <http://ontology.universAAL.org/ForaBloodpressureContextPublisher> ; a :ContextEvent ; rdf:subject <http://ontology.universAAL.org/InterIoT.owl#FIW43> ; :hasTimestamp "1497695335271"^^xsd:long ; rdf:predicate ns4:hasValue ; rdf:object _:BN000000 . :gauge a :ContextProviderType . <http://ontology.universAAL.org/ForaBloodpressureContextPublisher> a :ContextProvider ; :hasType :gauge . _:BN000000 a ns3:HeartRate , ns2:Measurement , ns3:HealthMeasurement ; ns2:value "101"^^xsd:int . <http://ontology.universAAL.org/InterIoT.owl#FIW43> a <http://ontology.universAAL.org/PersonalHealthDevice.owl#HeartRateSensor> , ns1:Device , ns1:PhysicalThing ; ns4:hasValue _:BN000000 .

En la Tabla 4.4 se puede ver la información de una medida de peso recogida por la báscula representada en una plataforma FIWARE utilizando el formado de datos

recomendado, mientras que en la Tabla 4.5 se puede observar cómo se representa esta misma información en la plataforma universAAL, después de efectuarse una traducción semántica. En la Tabla 4.6 se pueden observar las correspondencias entre los distintos conceptos clave, entre los cuales se puede establecer un alineamiento semántico. También es posible ver la traducción de una medida de pulsaciones desde FIWARE.

Tabla 5.6. Cuadro de conceptos y valores clave en la ontología origen (modelo de datos de FIWARE) y la ontología destino (universAAL). Se puede observar el resultado de la aplicación de la traducción semántica sobre la información.

	Modelo de datos de FIWARE (ontología origen)		**Ontología genérica de universAAL (ontología destino)**	
	Campo	***Valor (muestra)***	***Campo***	***Valor (muestra)***
ID de dispositivo	id	device:FIW:LD:test001	http://www.w3.org/1999/02/22-rdf-syntax-ns#subject	http://ontology.universAAL.org/InterIoT.owl#FIW33
Tiempo de medida	timestamp	2017-06-17T07:21:24.238Z	http://ontology.universAAL.org/Context.owl#hasTimestamp	1497694884238
Magnitud medida	quantityKind	weight	http://ontology.universaal.org/Measurement.owl#type	ns1:http://ontology.universAAL.org/InterIoT.owl#weight
Valor	value	73	http://ontology.universaal.org/Measurement.owl#value	73.0
Unidad	measurementUnit	kilogram	ns2:hasPrefix ns2:hasUnit	http://ontology.universAAL.org/Unit.owl#kilo http://ontology.universAAL.org/Unit.owl#gram

Igualmente al caso anterior, esta extensión para FIWARE puede incluir fácilmente otros sensores y tipos de medidas.

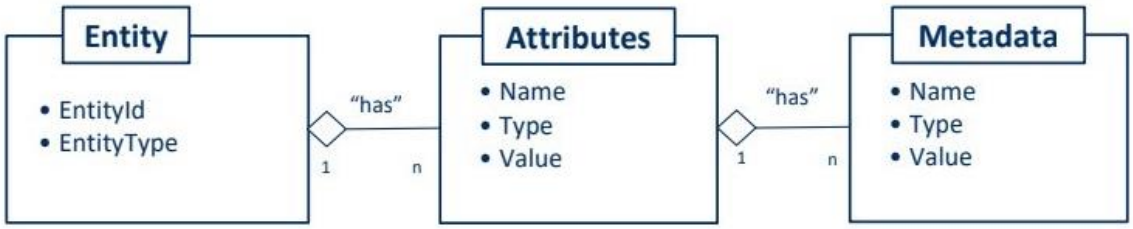


Figura 5.5 – Estándar NGSI v2 para el modelado de datos en FIWARE (fuente Modelado FIWARE [202]**)**

5.5.1.3 *Beneficios obtenidos*

El principal beneficio del sistema IoT propuesto consiste en la disponibilidad de una plataforma IoT sanitaria más potente para la monitorización del estilo de vida que puede implementar nuevas aplicaciones y servicios que las plataformas individuales no podrían soportar. Por otro lado, el proceso de monitorización puede descentralizarse del centro sanitario hasta los hogares de los sujetos monitorizados, permitiendo la monitorización contínua y remota de los sujetos, bajo observación profesional en todo momento, además de poder monitorizar elementos bajo movilidad fuera de recintos (centro de salud o domicilio) como indicadores de actividad física haciendo deporte. Esta monitorización móvil se consigue mediante la creación de redes de sensores corporales en los sujetos del programa, creando un novedoso entorno IoT móvil totalmente integrado en el sistema de seguimiento.

La aplicación del sistema de sistemas IoT INTER-Health para la monitorización y seguimiento de personas en el programa reduciría tanto los costes de traslado de los pacientes al centro médico como los tiempos de espera, obteniendo además resultados constantemente actualizados para realizar los ajustes necesarios de forma más rápida y precisa.

Desde la perspectiva del usuario final, el sistema INTER-Health proporciona beneficios muy significativos:

- Para los sujetos siguiendo el programa: mejorar la calidad del seguimiento sobre su estado de salud; mejorar la definición de los comportamientos de

riesgo; proporcionar información sobre las dietas y la actividad física más relevante con el estado de salud y con los riesgos del sujeto en comparación con los métodos tradicionales; aumentar la sensibilidad para el cribado de los sujetos que necesitan una intervención del médico local o de los hospitales (obesidad de segundo y tercer nivel, diabetes, etc.); reducir el tiempo de contacto presencial con el paciente ambulatorio nutricional y el número de desplazamientos.

- Para los servicios de salud pública: aumentar la eficiencia con los mismos recursos utilizados por utilizar monitorización continua; aumento de eficacia mediante la estandarización de las mediciones objetivas y subjetivas; convertir las subjetivas, como la práctica de la actividad, en objetivas (explotando los sistemas wearables de IoT); ampliar el número y el tipo de sujetos que recurren al programa nutricional.
- Para los médicos locales: aligerar la toma de cargo de los sujetos sanos por parte del médico local para garantizar una mayor disponibilidad hacia los sujetos patológicos (en conjunto, el médico local se convierte en un vehículo de una menor incidencia general de los costes sanitarios en la renta de los ciudadanos), mejorar la eficacia asistencial y diagnóstica poniendo la información actualizada directamente a disposición del médico en el sistema informático del médico local (es decir, los datos presentes en la plataforma utilizada del programa nutricional).

Este piloto validó la interoperabilidad semántica entre plataformas IoT heterogéneas mediante la solución de traducción semántica proporcionada por INTER-IoT, para lo cual hubo que conectar plataformas, utilizando el IPSM como elemento intermedio, y crear alineamientos específicos que habilitasen la traducción de la información compartida entre ellas.

Los alineamientos desarrollados se adaptaron y utilizaron en las casas inteligentes del despliegue del proyecto ACTIVAGE con fines de Envejecimiento Activo y Saludable (AHA). Así mismo, la extensión desarrollada permitiría conectar, por ejemplo, casas inteligentes para la tercera edad utilizadas en el ecosistema de ACTIVAGE utilizando

las plataformas SOFIA2 y FIWARE que empleen los modelos de datos vistos, permitiendo que utilizasen el sistema de monitorización para el programa de adquisición de hábitos de vida saludables y control del peso. También permitiría la inclusión de otras plataformas de Hogar Inteligentes FIWARE y SOFIA2 que utilicen este tipo de sensores y modelo de datos. Además, sería posible la inclusión de nuevas plataformas mediante la creación de nuevas extensiones utilizando otros alineamientos de traducción.

Desde una perspectiva e-health y AAL el sistema de monitorización INTER-Health permitió una mejora del servicio proporcionado a los sujetos del programa de hábitos saludables, así como una mayor efectividad del programa en los sujetos, reflejado en un mayor impacto positivo en el a salud de estos y en el seguimiento y continuidad en el programa. Estos resultados se midieron mediante indicadores objetivos en los dos grupos de estudio, como reflejan los KPIs de análisis del piloto publicados en [D8.3].

5.5.2. Otros casos de validación de la interoperabilidad semántica

Además de en el piloto de salud Inter-Health, visto en la sección anterior, en el marco del proyecto INTER-IoT se hizo uso de la herramienta IPSM para establecer interoperabilidad semántica entre plataformas en distintos casos de uso reales en distintos dominios [203], que validaron esta solución de interoperabilidad, así como la habilitación de interoperabilidad semántica entre plataformas heterogéneas:

- En el piloto Inter-LogP para el ámbito de transporte y logística portuaria. En concreto se interconectaron distintas plataformas de gestión portuaria, pertenecientes a entidades diferentes dentro del puerto (Terminal de contenedores, Autoridad Portuaria, Compañías de transporte terrestre) para permitir distintos casos de uso que requerían interoperabilidad a nivel de información entre ellos. De esta manera se pudo compartir información clave entre ellas para poder llevarlos a cabo, y mediante la solución semántica se pudo traducir esta información de manera que fuera entendible para la plataforma o el sistema que la recibía.

- En distintas aplicaciones en diversos proyectos de socios externos que colaboraban con el desarrollo de soluciones en IoT utilizando la solución de interoperabilidad semántica de Inter-IoT. Estos socios participaron en el proyecto Inter-IoT desde la convocatoria abierta de colaboración con el proyecto subvencionada por la Comisión Europea.
- Fuera del ámbito del proyecto Inter-IoT, se realizó también la validación de estas herramientas y métodos para proporcionar la interoperabilidad semántica entre plataformas heterogéneas en el proyecto LSP H2020 ACTIVAGE [175]. Esta aplicación de las soluciones de interoperabilidad semántica de Inter-IoT y su validación se verá en el próximo capítulo.

5.6. Ventajas de las soluciones y herramientas de interoperabilidad

Estas soluciones permiten cubrir las necesidades de las distintas capas de sistemas IoT heterogéneos gestionados por plataformas IoT, independientemente de que sigan estándares comunes que permitan una comunicación e interoperación directa. Es decir, ofrecen una solución alternativa al uso de estándares. La solución por uso de estándares tiene un ámbito y uso muy limitado y no es válida para la gran mayoría de plataformas en el ecosistema global IoT. Las herramientas para la interoperabilidad de INTER-IoT permiten establecerla entre distintas capas de sistemas heterogéneos. En el caso de la interoperabilidad entre plataformas a nivel de middleware y modelos semánticos de información, constituye prácticamente la única solución posible genérica y sistemática, a día de hoy, fuera del uso de estándares. Hay que destacar en este sentido:

- Enfoque capa a capa, soluciones independientes. Cubriendo la necesidades de la capa de dispositivo, red, middleware, semántica y aplicación.
- Traducción semántica universal: no conseguida con ninguna otra solución en IoT
- Evitar la fragmentación entre plataformas IoT e integrar horizontalmente silos verticales
- Posibilidad de permitir la comunicación entre plataformas

Aparte de su capacidad de proporcionar interoperabilidad entre sistemas y plataformas IoT heterogéneas, estas herramientas tienen características ventajosas:

- Virtualización: están virtualizadas para poder ser utilizadas de manera instántanea sobre cualquier sistema operativo y entorno para facilitar interoperabilidad. Previene los problemas de desactualización de librerías.
- Código abierto accesible, que permite su adaptación y extensión, y fomenta su adopción. Podría ser utilizado incluso con fines comerciales al estar bajo la licencia Apache Software Licence 2.0 [204].
- Programación en Java: la mayoría de herramientas, como el IPSM o Inter-MW, han sido programadas en Java, lo que permite que puedan ejecutarse sobre cualquier sistema operativo.
- Escalabilidad por diseño: permitiendo la conexión de múltiples elementos y el uso de torrentes de datos masivos, siendo apto para su uso en producción y
- Seguridad integrada: todas las APIs de herramientas pueden ser protegidas con tokens de seguridad y uso de TLS.
- Framework de integración y una metodología de implantación, para facilitar en la medida de lo posible su instalación, gestión y monitorización al usuario desarrollador.

5.7. Conclusiones

El proyecto INTER-IoT ha proporcionado un conjunto de herramientas que permiten habilitar la interoperabilidad en todas las capas de plataformas y sistemas IoT heterogéneos. Esto proporciona una serie de soluciones al complejo problema de la heterogeneidad y falta de interoperabilidad en IoT.

Estas soluciones siguen en general el enfoque de adaptación de elementos (semántica, formatos de datos, protocolos de red..) en lugar de uniformidad en los elementos (enfoque de uso de estándares comúnes. Este enfoque es en general más complejo que la simple adherencia a un estándar, en que los sistemas simplemente tienen que ser construidos (o inclusive adaptados) siguiendo un modelo establecido. La interoperabilidad por adaptación de elementos implica el añadido del estudio de varios modelos, estudio y diseño de formas de adaptarlos y transformarlos, y la

creación de elementos de adaptación. Además, también implican solventar el importante reto de tener que gestionar la adaptación de los grandes flujos de datos e información (IoT Big Data) en tiempo real.

Además, la heterogeneidad de los elementos a adaptar implica una gran complejidad en términos de diseño y desarrollo para poder realizar una adaptación potencial. Por ejemplo, los modelos de datos de IoT suelen no ser genéricos ni tener soporte para triples o anotaciones semánticas (RDF o OWL) lo que hace muy complicado poder transladar las relaciones a otro modelo o encontrar equivalencias o alineaciones entre ellos.

Pero en cambio, puede aportar grandes ventajas frente a las limitaciones de ámbito de la estrategia de uso de estándares comunes. La interoperabilidad basada en el enfoque de adaptación de distintos elementos entre los sistemas (ej. datos e información, formato de datos, modelo de información, semántica, protocolos..) puede aplicarse potencialmente a cualquier par de plataformas heterogéneas. Además, no limita la inclusión de nuevas plataformas a este grupo interoperable. En comparación, las plataformas a las que se podría aplicar interoperabilidad por uso de estándares es un conjunto muchísimo más restrictivo.

Las soluciones presentadas son en sí habilitadores digitales que permiten la interoperabilidad a distintos niveles en un sistema IoT y entre plataformas heterogéneas, las cuales no siguen un estándar entre sí. Se proporcionan elementos innovadores, como un traductor semántico universal de plataforma a plataforma, un middleware que permite la interconexión e interoperación de cualquier plataforma a nivel de middleware, a pesar de los estándares y formatos empleados, y una pasarela parcialmente virtualizada. La virtualización de las herramientas de interoperabilidad facilita su utilización en cualquier caso de uso, y su enfoque de soluciones independientes para cada capa de un sistema IoT hace que que se puedan aplicar de manera independiente unas de otras, y elegir el conjunto a utilizar, lo que proporciona más flexibilidad y adaptación a casos específicos en sistemas y plataformas IoT. También integran medidas de seguridad estándar. Es importante notar que algunas de estas soluciones genéricas requieren no solo se despliegue y configuración para un caso específico, sino también la programación de un trozo de software que recoge información de plataformas o entradas específicas, como sucede con el uso del IPSM

o Inter-MW (alineamientos y puentes). Estos desarrollos son necesarios para poder gestionar la situación de gran heterogeneidad entre los elementos. Al ser de dominio agnóstico (a diferencia de muchos estándares) estas herramientas pueden utilizarse para habilitar interoperabilidad para cualquier caso de uso y entre dominios de IoT en los que se requiera.

Estas soluciones se han validado en distintos dominios de aplicación en IoT, y a diferentes niveles o capas de un sistema IoT (dispositivo, red, middleware, semántica, aplicación). Como se ha visto en este capítulo se ha validado la habilitación de la interoperabilidad semántica entre plataformas en los pilotos de trasportes y logística portuaria. En esta línea, en el siguiente capítulo se estudiará el caso de uso real y validación de la aplicación de varias de estas soluciones en el dominio del Envejecimiento activo y saludable a gran escala en toda Europa, sobre plataformas de Hogares Inteligentes, probando su gran escalabilidad y así como el potencial de la interoperabilidad habilitada –y por tanto del uso de estas herramientas - para mejorar los servicios y proporcionar enormes beneficios al crear un ecosistema de plataformas y aplicaciones interoperable.

En especial, muy notablemente varias de estas herramientas (IPSM) son capaces de proporcionar interoperabilidad semántica entre plataformas de IoT heterogéneas que no comparten modelos de información, formatos de datos y semántica comunes y emplean interfaces de comunicación diferentes y heterogéneas. De esta manera, son la única solución existente en la actualidad para proporcionar interoperabilidad semántica entre plataformas heterogéneas. El IPSM constituye en este sentido un habilitador digital de interoperabilidad semántica entre plataformas IoT, capaz de proporcionar interoperabilidad semántica universal entre cualquier par de plataformas heterogéneas, y entre un conjunto de estas plataformas conformando un ecosistema de ellas.

Si bien existe la alternativa del uso de estándares comunes, su ámbito y posibilidades de aplicación son muy limitadas en la ausencia de un estándar global al que la gran mayoría de sistemas IoT y plataformas estén alineados, y no pueden aplicarse en general a plataformas heterogéneas.

La interoperabilidad en el IoT, y más concretamente entre plataformas, representa uno de los retos más importantes en IoT, el cual es solventado con esta solución de

interoperabilidad que permite la integración horizontal de silos verticales, puede evitar la fragmentación del ecosistema global IoT y permitir el desbloqueo de inmensos beneficios potenciales de la aplicación de la interoperabilidad entre sistemas., resolviendo problemas de la sociedad moderna para que la tecnología mejore la vida cotidiana de las personas e impulse la economía europea. Esta solución, como se ha visto, es de dominio agnóstico, y se puede aplicar a través de cualquier grupo de dominios. Esta solución no es conceptualmente brillante pero con las limitaciones de un prototipo a la hora de aplicarlo a situaciones de más envergadura que una traducción entre dos entidades con intercambios muy limitados de datos. Es capaz de gestionar múltiples traducciones y conversaciones entre plataformas simultáneamente de grandes torrentes masivos de información y datos IoT. Es destacable la capacidad y alcance que tiene esta solución para conformar ecosistemas interoperables de plataformas IoT, en los que cada plataforma puede intercambiar información con cualquier otra, entendiéndose el significado de la información recibida, y en los que existe flexibilidad a la hora de incluir o eliminar plataformas, gran capacidad de crecimiento, escalabilidad y coste lineal de inclusión de plataformas.

Además, la interoperabilidad es un elemento clave para la evolución de IoT y el paso a la nueva generación de Internet de las Cosas [19][205]: es esencial para la creación de interfaces humanas naturales en los sistemas de IoT, la existencia de entornos inteligentes ambientales o la integración de IoT con la inteligencia artificial, así como la creación de ecosistemas de plataformas completamente interoperables donde no haya barreras a la hora de comprender la información compartida por otra plataforma, aplicación u otra entidad. La falta de interoperabilidad actual es un freno a la evolución natural del IoT. En este sentido, el conjunto de herramientas de INTER-LAYER para proporcionar interoperabilidad en cualquier capa de un sistema o plataformas IoT puede ayudar a desbloquear esta situación de falta de interoperabilidad y permitir la evolución progresiva del IoT. En concreto, muy notablemente permiten la creación de ecosistemas interoperables de plataformas IoT heterogéneas.

Debido a su capacidad innovadora para proporcionar interoperabilidad completa entre plataformas IoT heterogéneas, que no siguen estándares comunes que

permiten su interoperación, junto a la facilidad de uso de su despliegue virtualizado, apertura de código y libre disponibilidad en la red, se espera la adopción futura de estas soluciones por desarrolladores, empresas y entidades de investigación para proyectos en los que sea necesaria la interoperabilidad en IoT – en especial a nivel de plataforma a nivel semántico.

Capítulo 6

Habilitación de la interoperabilidad semántica en ecosistema AHA de plataformas IoT

"Traducir es producir con medios diferentes efectos análogos."

Paul Valéry

6.1. Introducción

La actual barrera de falta de interoperabilidad entre plataformas IoT impide que los sistemas puedan interoperar entre ellos, compartir información valiosa y tener sinergias y cooperación entre ellos. Como ya se ha visto, la norma general es que plataformas que no fueron diseñadas no pueden interoperar y que exista una gran fragmentación en el ecosistema global IoT [8].

En el capítulo anterior se vio una solución innovadora y revolucionaria para habilitar la interoperabilidad semántica entre plataformas IoT heterogéneas, las cuales no son

capaces de interoperar directamente entre sí. Esta interoperabilidad estaba basadas en el uso de distintas herramientas que pueden proporcionar soluciones de interoperabilidad adaptadoras entre sistemas y capas de un sistema, las cuales pueden ser de inmensa utilidad en el fragmentado ecosistema actual de plataformas, entre las que destaca un traductor semántico (IPSM) [206].

Como ya se ha visto en capítulos anteriores, uno de los ámbitos donde el uso de sistemas IoT y la existencia de interoperabilidad entre ellos puede aportar mayores beneficios es en el ámbito médico y de Vida Cotidiana Asistida, intrínsecamente relacionados con el Envejecimiento Activo y Saludable (AHA) [2].

En este capítulo se describe un caso práctico de uso de dos de estas innovadoras soluciones de interoperabilidad (IPSM e Inter-MW) en despliegues de sistemas IoT a gran escala en Europa para el Envejecimiento Activo y Saludable en 9 países con miles de usuarios finales, con el objetivo de crear y promover el primer ecosistema AHA europeo dentro del marco del proyecto I+D H2020 ACTIVAGE [197][175]. La combinación del IPSM junto con Inter-MW crea una Capa de Interoperabilidad Semántica (SIL) integrada dentro de una suite de Interoperabilidad de Ecosistemas IoT (AIoTES)[207]. La aplicación de estas soluciones habilitando interoperabilidad semántica entre las distintas plataformas IoT de gestión AHA de Hogares Inteligentes permite importantes posiblidades técnicas fruto de la interoperabilidad y grandes beneficios.

Esta aplicación en un caso de uso real a gran escala, a diferencia de casos de uso desarrollados en el proyecto INTER-IoT, valida técnicamente la escalabilidad de las soluciones de interoperabilidad IPSM e Inter-MW ya que debe integrar un número muy elevado de plataformas IoT [175].

6.2. Planteamiento de creación de un ecosistema de plataformas AHA

Actualmente el envejecimiento de la población constituye un grave problema social, debido a la necesidad creciente de cubrir los cuidados especiales que necesitan, poder garantizar su bienestar y calidad de vida. La proporción de personas mayores de 65

años crece a gran velocidad en Europa año tras año y se calcula será una de cada seis personas en 2050 [163]. Los avances en bienestar y medicina permiten que la gente viva cada vez más años. La proporción de cuidadores frente a población envejecida y los métodos tradicionales para su cuidado no pueden cubrir estas necesidades de cuidados especiales, y la tendencia actual prevé que este problema se agravará en el futuro.

Frente a este problema, las nuevas tecnologías, y muy en especial IoT, pueden proporcionar soluciones tecnológicas para ayudar a un Envejecimiento Activo y Saludable, a mejorar el bienestar y calidad de vida de la población mayor y a fomentar un estilo de vida independiente.

En el marco del proyecto ACTIVAGE se han creado grupos independientes de Hogares Inteligentes en Europa con alrededor de 500 usuarios, especialmente diseñados para cubrir necesidades de usuarios mayores, persiguiendo su seguridad, bienestar y un estilo de vida saludable e independiente. Estos Hogares Inteligentes se apoyan en el uso de tecnología IoT y cada clúster o grupo independiente está gestionado por una plataforma IoT.

El conjunto de plataformas IoT que gestionan clústeres de Hogares Inteligentes o Despliegues AHA (DA) es muy heterogéneo en términos de tipo de plataformas utilizadas, modelos de representación de la información y formatos de datos en los que se soporta. Esto les impide interoperar entre ellas, compartir información valiosa y desarrollar sinergias como portabilidad de aplicaciones AHA.

El proyecto ACTIVAGE tiene como un objetivo principal permitir la interoperabilidad semántica en clústeres de Hogares Inteligentes a gran escala para la población mayor en 12 ciudades o regiones europeas y 9 países [175][191]. Cada uno de estos clústeres está gestionado por al menos una plataforma IoT, que gestiona la información proveniente de objetos inteligentes en los Hogares. Las razones por las que se tiene como objetivo crítico la habilitación de la interoperabilidad semántica son:

- La mejora de los servicios de AHA, debido a que la interoperabilidad entre sistemas puede dar lugar a beneficios muy notables.

- Promover la creación de un ecosistema IoT europeo creciente para el Envejecimiento Activo y Saludable. La falta de interoperabilidad es una barrera para tal fin.

Para ello se han definido inicialmente en el proyecto objetivos muy específicos de interoperabilidad, así como objetivos AHA que deben apoyarse a ser posible en los frutos de la consecución de la interoperabilidad entre DAs.

6.2.1. Objetivos de interoperabilidad

El desarrollo y despliegue técnico del proyecto ACTIVAGE busca satisfacer unos objetivos muy ambiciosos en términos de interoperabilidad para poder lograr un mejor servicio AHA y promover la creación de un ecosistema IoT europeo para fomentar el Envejecimiento Activo y Saludable, mejorando el bienestar y seguridad de ancianos y promoviendo una vida saludable e independiente.

Estos objetivos son:

- Permitir la portabilidad y reuso de aplicaciones y servicios entre DA por medio de la habilitación de interoperabilidad. Como ya se ha visto, las aplicaciones
- Interoperabilidad Inter-DA: Permitir la interoperabilidad semántica entre plataformas IoT de distintos DAs
- Interoperabilidad Intra-DA: Permitir la interoperabilidad semántica entre las distintas plataformas y sistemas IoT que pertenecen a un DA.
- Interoperabilidad entre DAs y sistemas o aplicaciones de terceros

6.2.2. Objetivos AHA

En el proyecto se definieron distintos objetivos AHA que debían ser cubiertos por los DA mediante la creación de servicios específicos [39]:

- La **monitorización de la actividad diaria** en el hogar para el apoyo de los cuidadores informales y para el seguimiento de los cuidadores formales con el fin de alertarles sobre las desviaciones de los hábitos de las personas mayores, permitiendo intervenciones tempranas mientras se amplía la independencia.

Los sensores inalámbricos, como los de presencia, contacto magnético, medición de potencia y proximidad, se despliegan en el hogar de los ancianos. Una pasarela transmite la información a una nube donde se realizan cálculos sobre actividades, tendencias y riesgos.

- **Atención integrada para adultos mayores con enfermedades crónicas**. Este caso de uso combina la monitorización de la actividad diaria en el hogar y el uso de dispositivos médicos para el seguimiento de la salud. La combinación de las tecnologías IoT con las soluciones de eHealth en un único sistema informático integrado, y la integración de los protocolos de atención de entidades que tradicionalmente trabajan por separado, promoverá la coordinación entre los proveedores de atención, la respuesta conjunta a las emergencias, una mejor planificación de los recursos y unas intervenciones más eficaces. Esto supondrá un ahorro económico y una mejor calidad de vida para las personas con enfermedades crónicas.
- **Monitorización de personas asistidas fuera de casa y control de situaciones de riesgo**. Este caso de uso combina dispositivos wearables, teléfonos inteligentes y la infraestructura de la Smart City para promover la socialización y la actividad. La infraestructura de la ciudad inteligente hace un seguimiento de los dispositivos portables y solicita ayuda si se cumplen determinadas normas para ayudar a las personas en riesgo.
- **Aviso de emergencia**. El sistema informa automáticamente de una emergencia cuando se detecta una situación crítica. Sensores inalámbricos o cableados y botones de "pánico" distribuidos en el entorno del hogar en situaciones estratégicas vinculados a una pasarela que reenvía la emergencia a un sistema de centro de llamadas. Otros escenarios complejos podrían implicar el procesamiento de datos en la nube privada o híbrida y luego la activación de la emergencia. En comparación con los sistemas de última generación en el hogar, la emergencia funciona cuando el usuario solicita ayuda, pero también cuando el entorno detecta la emergencia y la persona no puede (inconsciencia, caída, gas).

- **Promoción del ejercicio** para la prevención de caídas y la actividad física mediante el uso de sensores portátiles y ambientales.
- **Estimulación cognitiva** para la prevención del deterioro mental con el fin de prolongar el tiempo de vida independiente de las personas mayores. Este caso de uso combina la monitorización del comportamiento en casa y fuera de ella, y las intervenciones, como la promoción de ejercicios mentales y físicos y los juegos, haciendo uso de aplicaciones en tabletas o teléfonos inteligentes y dispositivos periféricos conectados.
- **Prevención del aislamiento social** mediante herramientas de comunicación en el hogar. Este caso de uso fomenta la interacción social y la movilidad mediante el uso de un sistema basado en vídeo y aplicaciones conectadas a la infraestructura de la ciudad inteligente, que proporciona datos sobre los eventos, y la vinculación con otros compañeros. Además, la continuidad entre el hogar (sensores domésticos) y los escenarios exteriores (el teléfono inteligente como sensor) proporciona información sin fisuras sobre la actividad social de los usuarios. El compromiso social aleja la depresión y el declive.
- **Confort y seguridad en el hogar**. Este caso de uso incluye el control del clima y la luz, la seguridad perimetral, el control de la energía y la automatización del hogar.
- **Apoyo al transporte y la movilidad**. Este caso de uso incluye la planificación de rutas adaptadas para personas mayores tanto en ciudades como entre distintas ciudades. Las rutas pueden calcularse haciendo uso de los datos de la ciudad inteligente sobre las condiciones del tráfico y otros aspectos de la movilidad, y personalizarse en función de objetivos como la promoción del ejercicio o la búsqueda de la ruta más fácil/rápida.

La habilitación de interoperabilidad semántica ente las distintas plataformas de gestión de DAs puede ayudar a la mejora del servicio AHA proporcionado por ellas, al permitir la cooperación y sinergias entre sistemas y la “portabilidad” de aplicaciones específicas para una determinada plataforma y modelo de información en el conjunto de DAs. Esto se verá en detalle a lo largo del capítulo.

6.2.3. Reto técnico de interoperabilidad

El grupo inicial de clústers de Hogares inteligentes estaba compuesto por 9 DAs en distintas ciudades o regiones europeas (Galicia, Madrid, Valencia, Grecia, Región de Emilia Romana, Isère, Leeds, Woquaz, Finlandia). Cada uno de estos despliegues de Hogares Inteligentes AHA está gestionado al menos por una plataforma IoT, y el conjunto de plataformas IoT que gestionan los distintos DA es muy heterogéneo como puede verse en la Tabla 6.1. Esto es así en términos de tipo de plataforma, interfaces de comunicación, formato de datos utilizado para almacenar la información y modelos semánticos de representación de la información.

Debido a sus diferencias respecto a su forma de representación de la información, estas plataformas no son interoperables entre sí y no es posible habilitar la interoperabilidad semántica directamente entre ellas. Además, otras diferencias entre ellas como sus distintas interfaces y procedimientos de comunicación dificultan la consecución de interoperabilidad.

Figura 6.1 Clústers iniciales de Hogares Inteligentes AHA

Además de la creación de un ecosistema inicial interoperable semánticamente de 10 plataformas IoT dentro de los objetivos del proyecto estaba la inclusión de 3 nuevos DA en el último tercio de vida del proyecto (Lisboa, Sofia y Cataluña), así como otros sistemas IoT gestionados por plataformas como los que se pudiesen crear en la

Primera Convocatoria Abierta de Colaboración del proyecto LSP H2020 ACTIVAGE. También se contemplaba la inclusión futura de otras plataformas y sistemas AHA que se quisieran adherir al ecosistema una vez finalizado el proyecto. En la Tabla 6.1 se pueden ver las características de los 3 últimos DAs a incorporar al ecosistema de plataformas.

Hay que destacar también el reto técnico que implica que la interoperabilidad semántica debe ser habilitada entre un número muy elevado de plataformas. Sin una solución escalable y con un coste de inclusión lineal, el aumento de la complejidad técnica sería exponencial, como sucede típicamente con soluciones ad hoc para permitir intercambios de datos entre plataformas no interoperables [Matilde, ver cual puso].

La creación de este ecosistema interoperable de plataformas IoT gestionando 12 DAs se llevó a cabo mediante el uso de una solución de interoperabilidad, AIoTES, con una arquitectura de interoperabilidad asociada. AIoTES o Suite de ACTIVAGE para la creación de Ecosistemas IoT está basada en el uso del traductor semántico IPSM, capaz de habilitar interoperabilidad semántica entre plataformas IoT, y su combinación con una herramienta complementaria para la gestión de la comunicación y recursos de plataformas: Inter-MW [208]. Ambas herramientas provienen del proyecto INTER-IoT para la interoperabilidad de plataformas IoT heterogéneas [209].

Este grupo de plataformas muy heterogéneo entre sí, reflejando la situación general de heterogeneidad entre plataformas y sistemas IoT. El ecosistema de plataformas a crear durante el tiempo de vida del proyecto ACTIVAGE contenía 13 plataformas de gestión AHA de grupos de Hogares Inteligentes y e inclusive un sistema IoT de salud. En este conjunto se incluían instancias de los siguientes tipos de plataforma: FIWARE [62], SOFIA2 [68], universAAL [63], sensiNact [65], OpenIoT [210], IoTivity [49] , MC Cardio [211], ekenku [212], ekauri [213], openHAB [214]. Un requerimiento de ecosistema era la posibilidad de incorporar nuevas plataformas IoT al ecosistema inicial creado, y en este sentido se pretendía que las plataformas de la Segunda Convocatoria Abierta de Colaboración del proyecto fueran añadidas en un segundo periodo. En ese sentido las plataformas MC Cardio [211], ekenku [212], ekauri [213],

openHAB [214] debían ser incorporadas en el último tercio de vida del proyecto al grupo inicial.

Tabla 6.1 DAs iniciales y tipo de plataforma IoT de gestión

DA iniciales	Tipo de Plataforma IoT
Galicia (España)	SOFIA2
Valencia (España)	FIWARE
Madrid (España)	universAAL
Region Emilia Romana (Italia)	FIWARE
Grecia	universAAL
Isere (Francia)	sensiNact
Woquaz	universAAL
Leeds (Reino Unido)	FIWARE
Finlandia	universAAL

Tabla 6.2 DAs iniciales y tipo de plataforma IoT de gestión

DA finales	Tipo de plataforma IoT
Sofia (Bulgaria)	OpenHAB
Lisboa (Portugal)	FIWARE
Cataluña (España)	ekenku, ekaurii

6.3. Arquitectura de Interoperabilidad para AHA

En el proyecto LSP H2020 ACTIVAGE se ha diseñado una arquitectura de interoperabilidad con el objetivo de crear un ecosistema interoperable a gran escala de plataformas de gestión AHA. Esta arquitectura busca conectar las distintas

plataformas y satisfacer las necesidades y objetivos de interoperabilidad en ellas y entre ellas ya definidos en la sección anterior, garantizando la seguridad y la privacidad de la información fluyendo a través de ella. Además, esta arquitectura ofrece una capa de herramientas y servicios diversos que pueden ser útiles para los gestores de las plataformas.

Para ello se ha desarrollado e integrado la suite de interoperabilidad AIoTES [207], que permite la conexión de plataformas y la interoperabilidad semántica entre ellas. El elemento que proporciona interoperabilidad entre las plataformas conectadas es la SIL, compuesto por dos herramientas vistas en el capítulo anterior: el traductor semántico IPSM y el middleware de plataformas Inter-MW. Su uso combinado resuelve la comunicación con las plataformas y el IPSM, además de la adaptación del formato sintáctico de los datos y mensajes recibidos o enviados a las plataformas.

Otros elementos en AIoTES son un conjunto de herramientas técnicas que pueden resultar de utilidad a gestores de plataformas y un módulo de seguridad basado en la herramienta de código abierto KeyCloack [215], el cual siguiendo mecanismos estándar proporciona gestión de seguridad OATH 2.0 [216] en la suite, conjuntamente con una pasarela-API.

Las plataformas pueden conectarse a esta suite de interoperabilidad, permitiendo interoperabilidad entre ellas y entre las aplicaciones asociadas a ellas a diferentes niveles. De esta manera se establece una arquitectura de interoperabilidad compuesta por las siguientes capas: Dispositivo, Plataforma, Capa de Interoperabilidad Semántica (SIL), Capa de Servicios, Capa Transversal de Seguridad y Privacidad y Capa de Aplicaciones.

Esta arquitectura es el fruto del trabajo conjunto de diferentes socios y entidades en el proyecto ACTIVAGE.

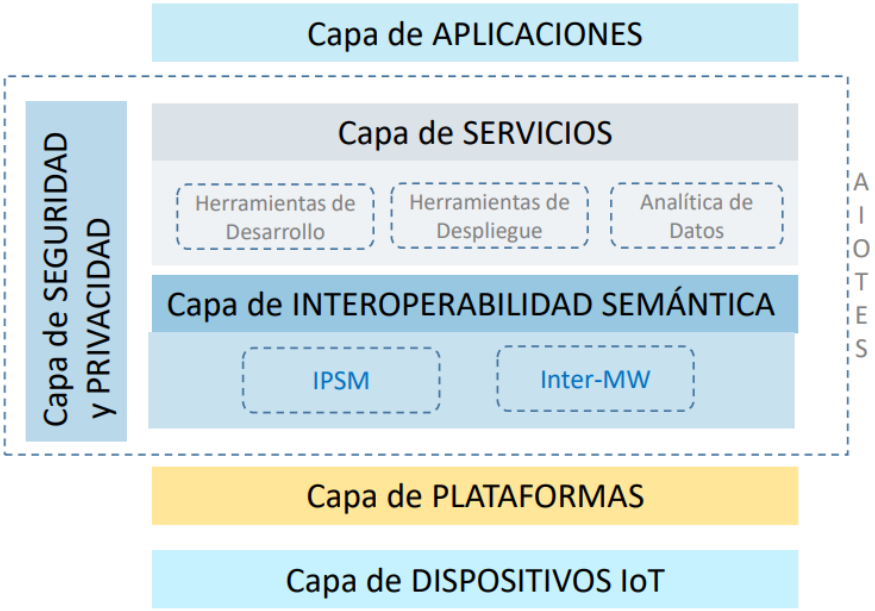


Figura 6.3 Arquitectura AHA de Interoperabilidad del proyecto ACTIVAGE

6.3.1. AIOTES

Como se ha visto en la descripción de la arquitectura, la Suite para Ecosistemas IoT de ACTIVAGE (AIoTES) [39][207] es un framework que proporciona interoperabilidad entre plataformas, además de garantizar la seguridad y privacidad en su acceso y uso (incluyendo el intercambio de información IoT) y de proporcionar herramientas útiles a gestores de plataformas AHA. Desde el punto de vista de la interoperabilidad IoT entre plataformas el componente responsable de su habilitación es el conjunto complementario del IPSM con Inter-MW o SIL.

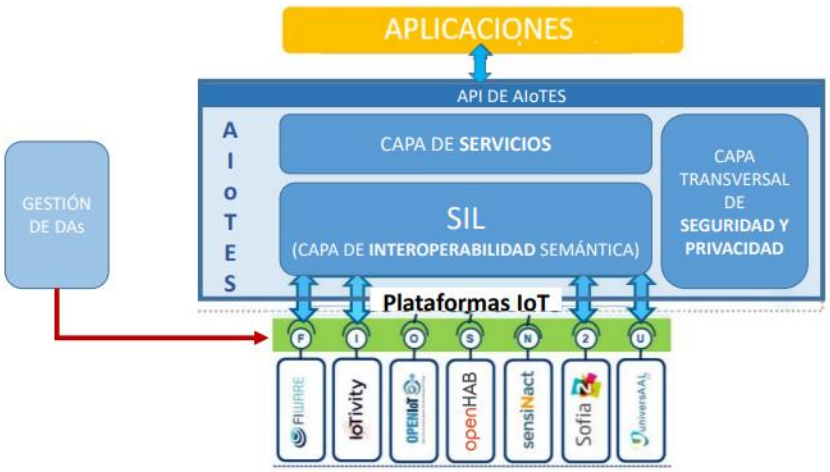


Figura 6.3 Esquema básico de los bloques componentes de AIoTES

Su arquitectura y distribución en distintos bloques funcionales puede verse en la Figura 6.3. AIoTES está compuesto por los siguientes bloques funcionales:

- Capa de Interoperabilidad Semántica (SIL) compuesta por la versión 8.8 del IPSM y la versión 2.3.1 de Inter-MW.
- Capa de Servicios, que contiene herramientas que podrían resultar útiles a desarrolladores de aplicaciones para AIoTES, aplicaciones AHA en general o para gestores de plataformas AHA o de la suite AIoTES. Las herramientas serían de distinto tipo:
    - Desarrollo: proporcionan algún tipo de asistencia o soporte para la realización de determinados desarrollos SW relacionado con AIoTES.
    - Despliegue: ayudan a desplegar distintos elementos SW.
    - Gestión de la SIL, relacionadas parcialmente con el desarrollo de aplicaciones.
    - Analítica de Datos.
- Módulo de Seguridad y Privacidad, que aporta una capa transversal de privacidad y seguridad al sistema adicional a la garantizada por los

componentes y los otros bloques funcionales individualmente. Se basa en el uso de medidas de seguridad estándar (autenticación, conexión segura, uso de tokens de seguridad, estándar OATH 2.0 y gestión de distintos elementos de seguridad desde la herramienta KeyCloack).

- Capa de Gestión de DAs, externa e independiente al resto del framework, que proporciona monitorización de Indicadores de Puntos Clave (KPIs) de cada DA adscrito.

El Marketplace de ACTIVAGE representa un componente externo a la suite, pero intrínsecamente relacionado con ella que se puede desplegar en un servidor externo con el fin de almacenar, gestionar y proporcionar aplicaciones del ecosistema AHA.

La suite presenta las siguientes interfaces:

- El API de AIoTES, que engloba las APIs individuales de los componentes y permite la obtención de información IoT de los DAs entre otras muchas funciones.
- Los puentes de plataforma de Inter-MW (SIL) a los que se conectan las plataformas IoT.
- Una interfaz gráfica de gestión de despliegue de componentes.

6.3.2. Capa de Interoperabilidad Semántica

La Capa de Interoperabilidad Semántica (SIL) permite la interoperabilidad a nivel semántico entre plataformas de IoT, y entre plataformas y aplicaciones u otro tipo de entidad consumidora o productora de datos que esté conectada a AIoTES. La SIL está compuesta por dos elementos del proyecto INTER-IoT: la combinación del traductor semántico IPSM [206] junto con el middleware de plataformas Inter-MW [208]. Su uso combinado permite realizar las conversiones y adaptaciones necesarias para permitir un entendimiento común entre la plataforma emisora de la información y la receptora, además de gestionar la comunicación con las plataformas, proporcionando interoperabilidad semántica y sintáctica [208][8]. De este modo, el formato sintáctico y la semántica específicos de la plataforma o de AIoTES se convierten en el formato y

la semántica del receptor correspondiente, manteniendo el significado de la información.

Como se ha visto en el capítulo 5, proporciona mecanismos escalables de interoperabilidad entre plataformas que implican un coste drásticamente menor que una conexiones directas entre plataformas. Desde el punto de vista de la privacidad, crítica en entornos AHA, las plataformas deciden la información que se comparte con usuarios consumidores autorizados (normalmente plataformas y aplicaciones externas).

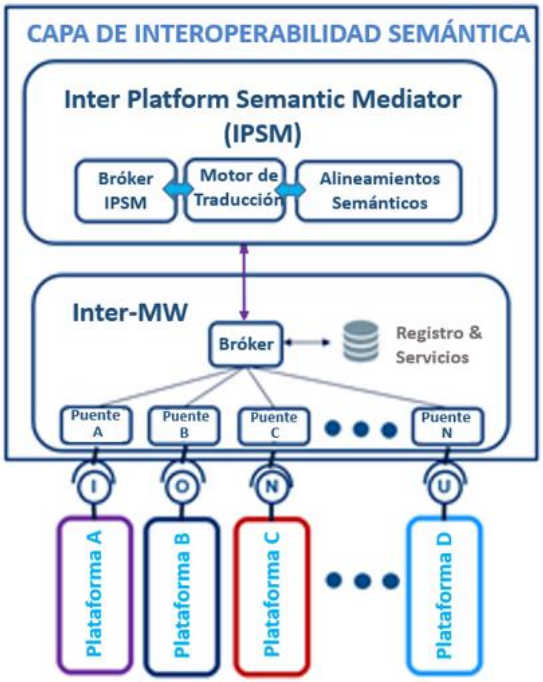


Figura 6.3 Componentes del SIL y conexión de plataformas

6.4. Desarrollo de Software para la Interoperabilidad

Fue necesario efectuar determinados esfuerzos de desarrollo en el marco del proyecto ACTIVAGE para la creación de AIoTES y para la integración de plataformas y sistemas IoT utilizando esta suite.

Para la integración de las plataformas IoT fue necesario realizar determinados desarrollos:

- La creación de puentes de Inter-MW para habilitar la conexión
- La creación de alineamientos semánticos específicos para cada DA o instancia de plataforma de gestión.

Además de los esfuerzos realizados para la integración de plataformas IoT de DAs, en la Primera Convocatoria de Colaboración Abierta con el proyecto (1st Open Call) se realizaron desarrollos específicos para poder integrar soluciones AHA en el ecosistema.

Otro desarrollo en el proyecto relacionado con la interoperabilidad semántica fue el desarrollo de una ontología específica para AHA, muy relevante en el diseño de alineamientos.

Por otro lado, hay que notar que para la creación del framework para la ineroperabilidad de DAs, AIoTES, se llevó a cabo el desarrollo de múltiples componentes aparte de la creación de puentes para Inter-MW. Aunque la SIL estaba compuesta por herramientas ya existentes, y el MSP estaba basado en la herramienta de código abierto KeyCloack, fue necesaria la creación de distintas herramientas componiendo la capa de servicios. También fue necesario cierto esfuerzo de desarrollo en el proceso de integración, descrito de manera general en otra sección dedicada al proceso de integración del framework AIoTES.

6.4.1. Desarrollo de puentes

Para poder conectar a la SIL plataformas de un determinado tipo (p.e. FIWARE, universAAL o sensiNact) es necesario instalar previamente en Inter-MW una pieza de software llamada ***puente*** específicamente diseñado para este tipo de plataforma [217]. Este puente es una parte de Inter-MW instalable como módulo y permite:

- La comunicación bidireccional entre Inter-MW y cualquier instancia de ese tipo de plataforma. Esta comunicación solo implica gestión de recursos y envío de datos, pero no interoperabilidad semántica. Pueden conectarse a él y

utilizarlo simultáneamente múltiples instancias del tipo de plataforma concreto para la que se ha construido.

- La conversión de la sintaxis o formato de datos en que maneja la información la plataforma y el formato de Inter-MW (JSON-LD), lo que permite la interoperabilidad sintáctica

Por extensión, al permitir la comunicación bidireccional con la SIL, los puentes permiten la comunicación entre la plataforma y otras plataformas, aplicación u otra entidad conectada a través de ella.

Los puentes de comunicación además pueden soportar funciones de seguridad como TLS o autenticación de plataforma si están adecuadamente diseñados para ello.

En el caso de que no se disponga del puente necesario para un tipo de plataforma concreto que se quiera conectar, es necesario desarrollarlo. El puente se crea a partir de un proyecto Maven en Java, que una vez compilado da lugar a un fichero JAR instalable en Inter-MW [218][217]. Para su construcción es necesario:

1) Añadir las dependencias necesarias de Maven (hay 3 obligatorias que proporciona Inter-MW). Si hacen falta dependencias extra deben ser añadidas.
2) Implementar las clases abstractas necesarias en la plantilla Java para la creación de un puente. Esta plantilla está proporcionada por el proyecto INTER-IoT en su documentación disponible en línea como código abierto [219]. Las dos clases principales son:
    - *Implementación del puente*, que habilita la comunicación entre la plataforma e Inter-MW y debe implementar la interfaz del puente extendiendo la clase abstracta abstractBridge e implementando sus métodos.
    - *Translator*, responsable de la conversión de formatos sintácticos (entre el formato de datos utilizando en la plataforma a conectar a JSON-LD, el formato de datos de Inter-MW). Esta conversión debe poder realizarse de manera bidireccional. Esta clase no es necesaria si el

formato de plataforma es RDF, ya que en ese caso el cambio de serialización es realizado por Inter-MW.

3) Finalmente debe ser testeado con tests unitarios (JUnit) y de integración proporcionados por el proyecto INTER-IoT para tal fin [217] en su documentación online, e instalado como JAR en Inter-MW para comprobar su funcionalidad.

Métodos de la interfaz de puente

El bridge debe implementar los siguientes métodos en la clase de implementación que conforman su interfaz de puente, que deben cumplir con la funcionalidad descrita:

- **registerPlatform:** registro de la plataforma especificada en Inter-MW asociada a un puente específico y creación de una instancia virtual de plataforma.
- **updatePlatform:** actualización de un registro en Inter-MW de una plataforma especificada.
- **deletePlatform:** anulación del registro de la plataforma especificada.
- **subscribe:** creación de una suscripción a información IoT del dispositivo seleccionado al cliente a las observaciones generadas por un dispositivo IoT gestionado por una plataforma. El método subscribe debe implementar un listener que acepte los mensajes de observación enviados desde la plataforma a Inter-MW para su correspondiente suscripción. El listener se implementa utilizando el framework Spark. Escucha en el puerto definido por la propiedad de configuración bridge.callback.url (8980 por defecto) y la ruta que coincide con el parámetro conversationId. En el método handler (callback) los datos de observación se convierten en un mensaje de observación de tipo Message y se envían a través de Inter-MW.
- **unsubscribe**: cancelación de una suscripción especificada a información IoT que había sido creada con el método *subscribe*.
- **query:** realización de una consulta sobre el estado y la última observación realizada por un dispositivo especificado.
- **listDevices**: lista todos los dispositivos detectados por la plataforma. Realiza una consulta a la plataforma para obtener todos los dispositivos gestionados

por ella que considere detectables. Es invocado por Inter-MW para realizar las funciones de descubrimiento de dispositivos (*deviceDiscovery*)

- **platformCreateDevices:** instrucción para que una plataforma comience a gestionar (es decir, crear) un nuevo dispositivo.
- **platformUpdateDevice:** ejecuta la instrucción para que una plataforma actualice la información sobre un dispositivo conectado y gestionado por ella
- **platformDeleteDevice: i**nstrucción para que una plataforma deje de gestionar (es decir, elimine) un dispositivo.
- **observe:** envía un mensaje de observación desde Inter-MW a la plataforma (el puente actúa como editor para la plataforma).
- **actuate:** similar a Observe pero portando instrucciones de actuación para un actuador.
- **error:** devuelve un mensaje de información sobre cualquier error ocurrido dentro del puente o dentro de Inter-MW.
- **unrecognized:** devuelve información de error sobre mensaje recibido cuyo tipo o formato no es reconocido por Inter-MW .

Tabla 6.3 con métodos abstractos a implementar de la clase AbstractBridge

Message **listDevices**(Message message) throws Exception;
Message **query**(Message message) throws Exception;
Message **platformCreateDevices**(Message message) throws Exception;
Message **platformUpdateDevices**(Message message) throws Exception;
Message **platformDeleteDevices**(Message message) throws Exception;
Message **observe**(Message message) throws Exception;
Message **actuate**(Message message) throws Exception;
Message **error**(Message message) throws Exception;
Message **unrecognized**(Message message) throws Exception;

Resultados del desarrollo de puentes

En el marco de esta tesis doctoral se ha colaborado en la actualización, testeo y desarrollo de puentes de comunicación de plataformas. En especial se ha participado, además de soporte técnico y testeo, en el diseño/desarrollo de la parte generalmente

más compleja del desarrollo de los puentes, el traductor sintáctico o *translator*, en el puente para el sistema MC CARDIO [211], el cual permite el envío de señales de electrocardiograma (ECG). Este tipo de adaptador sintáctico capaz de convertir la sintaxis a JSON-LD fue diseñado de manera especial para hacer que pudiera generar el mensaje RDF expresado directamente, de forma nativa, con la ontología AHA de ACTIVAGE. Esta funcionalidad extra solo es posible añadirla sobre un puente en determinados casos muy especiales y atípicos de sistemas IoT invariantes. El sistema solo generaba un tipo de mensaje invariable en cualquier instancia existente o futura, a diferencia de una plataforma IoT convencional. Su desarrollo fue complejo y permitió que enviase directamente la información del ECG en el modelo semántico de ACTIVAGE, la ontología AHA basada en GOIoTP.

También se hizo un análisis de la clase *translator* del puente de sensiNact para el análisis de su modelo de datos tras el uso del bridge. Este puente altera la semántica del modelo de datos inicial de sensiNact aportando una estructura final bastante compleja sin realizar ninguna traducción o mapeo.

Dentro del proyecto se reutilizaron, actualizaron o desarrollaron 8 puentes para poder conectar 7 plataformas diferentes (FIWARE, SOFIA2, IoTivity, sensiNact, universAAL, OpenIoT, openHAB) además del sistema IoT MC CARDIO. El puente OpenHAB [214] fue desarrollado para la revisión final de proyecto de INTER-IoT y solo estuvo disponible posteriormente a la fase de preparación de puentes de ACTIVAGE.

6.4.2. Desarrollo de alineamientos

En el marco de esta tesis doctoral se participó de forma muy relevante en el desarrollo de alineamientos. Se lideró esta tarea y se proporcionó directrices y soporte técnico a los distintos DA y socios externos que querían desarrollarlos. Se ha participado en el desarrollo de todos los alineamientos desarrollados en el proyecto ACTIVAGE, colaborando con los socios responsables de su desarrollo en los DAs. En concreto, se han desarrollado en su totalidad los alineamientos para el DA de Galicia, para un testbed de FIWARE y para un testbed de universAAL.

Tabla 6.4 Distintos alineamientos desarrollados en el proyecto ACTIVAGE.

Despliegue AHA	Tipo de plataforma	Alineamientos
DA Valencia	FIWARE	Unidireccional
DA Galicia	SOFIA2	Bidireccionales Extensión servicio corazón Grecia (doble: subida y bajada) Extensión recepción señal MC Cardio
DA Leeds	FIWARE	Bidireccional* Extensión recepción señal MC Cardio
DA Isere	sensiNact	Bidireccional Extensión con un bug que arreglar para la recepción de información sobre sensor de cama de presión Extensión para soportar la recepción de la información del sistema MUVONE
DA Darmstad	universAAL	Bidireccional Extensión
Alineamientos Genéricos de universAAL	universAAL	Bidireccional Soportan las ontologías genéricas de universAAL Bug menor por arreglar en el descencente
DA RER (Región Emilia Romagna)	FIWARE	Unidireccional Información codificada que representaba un reto de transformación dentro del alineamiento (cambio de cadenas)
DA Finlandia	universAAL	Bidireccional Soportan la información gestionada por la plataforma universAAL del DA

DA Madrid	universAAL	Bidireccional Extensión de los alineamientos genéricos para universAAL incluyendo las extensiones particulares de las ontologías realizadas en esa instancia de plataforma universAAL
DA Grecia	universAAL	Bidireccional Extensión de los alineamientos genéricos para universAAL incluyendo las extensiones particulares de las ontologías realizadas en esa instancia de plataforma universAAL Extensión para el uso del sistema SmartFloor y MUVONE
DA Grecia II	FIWARE	Bidireccional Soporta la recepción del sistema MUVONE
DA Lisboa	FIWARE	Unidireccional
DA Cataluña	eukari	Bidireccional
DA Cataluña II	eukendu	Bidireccional
DA Sofia	OpenHAB	Unidireccional
Testbed OpenIoT	OpenIoT	Bidireccional
Testbed FIWARE	FIWARE	Bidireccional
Testbed IoTivity	IoTivity	Bidireccional Publica la información de 3 tipos de medidas: luminancia, presencia y pulsaciones
Testbed universAAL	universAAL	Unidireccional Soporta la información de 5 medidas médicas.

		Utilizado en una demostración para la revisión técnica del proyecto
Sistema IoT Muvone	MUVONE	Unidireccional No tenía sentido bidireccional, envía información que debe ser recibida y gestionada en un DA
Sistema IoT SmartFloor	universAAL	Unidireccional No tenía sentido bidireccional, envía información de un sensor concreto a una aplicación sobre AIoTES y al conjunto de plataformas para utilizar servicios útiles relacionados.
Extensiones para MC CARDIO	SOFIA2	Soporte para la recepción de la señal ECG del sistema MC CARDIO Alineamientos simples para la conexión del sistema MC CARDIO

Aunque se pueden desarrollar un gran número de alineamientos para un sistema o plataforma IoT, lo óptimo es ampliar si es necesario el empleado para la traducción de la plataforma a AIoTES y el utilizado para la traducción en el sentido contrario, y utilizar solamente dos. La ampliación puede ser necesaria si se incluyen nuevos tipos de información a recibir o a publicar (p.e. se incorporan nuevos tipos de sensores en el despliegue AHA que hay que incluir en el modelo de datos u ontología de la plataforma).

Es imprescindible que cada DA desarrolle un alineamiento para traducir la información que quiera publicar, para que así pueda ser utilizada por servicios en otros DA (pudiendo beneficiarse de ellos) o bien por aplicaciones sobre AIoTES que utilizan información IoT en el modelo semántico de información de ACTIVAGE, y son por tanto multiplataforma (mediante el uso de la SIL). El DA decide cuándo y cómo comparte esta información, y sobre cuáles sensores y usuarios se genera, así como las restricciones de privacidad aplicadas.

En el caso de los de alineamientos para la recepción de datos, cada DA fue creando y adaptando su alineamiento desde AIoTES hacia la plataforma según sus necesidades. Algún DA consideró innecesario su uso ya que no tenían planeado utilizar información externa, pero por norma general la gran mayoría de DAs lo implementaron.

El proceso para su desarrollo y uso ha sido descrito en un capítulo anterior. Se utilizó la estrategia de uso de una ontología central para permitir su publicación en un modelo semántico común desde el API y por razones de escalabilidad y gestión de traducción.

Se llevó a cabo un mecanismo de testeo gradual a lo largo del desarrollo de los alineamientos, considerándose finalizados una vez comprobado que efectuaban correctamente traducciones semánticas para el conjunto de información que compartían o recibían.

Hay que notar que a diferencia de los puentes, que son módulos de Inter-MW, los alineamientos no forman parte de la SIL o de AIoTES. En su lugar son un código de programación semántica para la traducción, específico para el modelo de información de un DA o plataforma IoT que quiera añadirse al ecosistema interoperable. No se pueden considerar parte del framework aunque su diseño y creación es un requisito esencial para poder utilizarlo, conectar las plataformas a él y habilitar la interoperabilidad semántica. Es el único requisito de desarrollo que debían llevar a cabo los DA, plataformas o sistemas IoT que quieran integrarse en el ecosistema interoperable en ACTIVAGE. Si bien sería necesario el desarrollo de puentes en el caso de no estar disponibles para el tipo genérico de plataforma del DA, en el caso concreto del proyecto ACTIVAGE los puentes fueron creados previamente por desarrolladores responsables del tipo de plataforma. Las plataformas de los clústers de Hogares Inteligentes solo reutilizaron los puentes disponibles de INTER-IoT o los desarrollados en ACTIVAGE.

6.4.3. Desarrollo de herramientas

En el marco de esta tesis doctoral se han desarrollado varias herramientas relacionadas con el uso de la SIL y la interoperabilidad, y se ha contribuido a la

integración de los mecanismos de seguridad y privacidad OATH 2.0 y autenticación de la Capa de Servicio mediante la creación y aplicación de scripts específicos de uso general en ella.

Se ha desarrollado la herramienta SIL-subscriber o SIL TOOL, que permite la suscripción a la información IoT generada por dispositivos concretos seleccionados (sensores o bien "sensores virtuales" que representan a una aplicación o servicio cuyos datos son gestionados por la SIL). Esta suscripción puede hacerse mediante una serie de llamadas al API de la SIL (integrada dentro del API de AIoTES) y resulta un proceso largo y complejo a la hora de realizarse manualmente por una persona. La aplicación La información se recibe en el formato común de Inter-MW y el IPSM (JSON-LD) y representada mediante el modelo semántico de la ontología de ACTIVAGE. Esto permite la utilización y explotación de la información IoT semánticamente homogénea fruto de la interoperabilidad semántica entre plataformas, en servicios y aplicaciones por parte de gestores de plataforma, desarrolladores, y usuarios no técnicos. Por ejemplo, permite la conexión de información IoT de sensores a un servicio de análisis de Big Data mediante el envío de una suscripción al punto de acceso del servicio o aplicación o una aplicación multiplataforma.

Otra herramienta que se ha desarrollado que muy relacionada con la interoperabilidad de plataformas es el IDE para desarrolladores de AIoTES, que integra distintas herramientas. Estas permiten o facilitan la labor a técnicos para realizar desarrollos concretos relacionados con AIoTES. Una de estas herramientas permite la creación rápida, guiada y visual de aplicaciones AHA combinando respuestas de sensores con acciones específicas sobre actuadores y avisos o alertas, monitorizando la información y presentando cuadros de información solicitados. Para ello, esta herramienta obtiene automáticamente la información recogida por los sensores desde la SIL. También contiene una herramienta que permite la creación de secuencias o flujos de ejecución basada en NODE-Red, la cual permite la explotación de datos de sensores IoT, y la combinación funciones de preprocesamiento y uso de aplicaciones. Por último, otra de estas herramientas facilita el desarrollo tanto de puentes como de alineamientos semánticos proporcionando plantillas de programación adecuadas para el caso de aplicación y uso concreto. El IDE tiene una

Interfaz Gráfica de Usuario (GUI) de gran usabilidad y, además de ofrecerse integrado en el framework de AIoTES, ofrece una versión virtualizada que se puede desplegar en instantes en cualquier ordenador independientemente del sistema operativo sin requerir ningún tipo de configuración.

Estas herramientas se virtualizaron utilizando la tecnología Docker y Docker-Compose, y se les integraron mecanismos de seguridad específicos de AIoTES (autenticación, uso de tokens, integración con KeyCloack, seguridad OATH 2.0 en backend, interacción con la API de AIoTES) que posibilitaron su inclusión en el framework garantizando las especificaciones de seguridad y privacidad de AIoTES al respecto.

6.4.4. Desarrollo para la inclusión de soluciones de la Convocatoria Abierta de Colaboración

En la Primera Convocatoria Abierta de Colaboración del proyecto LSP H2020 ACTIVAGE (1st Open Call) se seleccionaron 10 propuestas de proyectos de socios externos para ofrecer múltiples soluciones AHA en el ecosistema ACTIVAGE, para lo que era necesario que estuviesen técnicamente integradas con AIoTES. En el marco de esta tesis doctoral se con todos los miembros de la desde un punto de vista técnico y se participó en el diseño inicial de integración, proporcionando opciones y guía para su integración. También se les proporcionó soporte técnico respecto al uso e integración con la SIL (instalación, uso general, desarrollo de puentes y alineamientos). Se colaboró muy activamente con 3 grupos de los 10 seleccionados, cuyo desarrollo estaba muy enfocado en el uso de la SIL, contribuyendo en su integración:

- MC Cardio: este grupo integró un sistema de monitorización de electrocardiogramas (ECM) pudiendo enviar la señal recogida por el dispositivo médico a través de la SIL. Se realizó un puente para conectar su sistema IoT a la SIL con un diseño del método de adaptación sintáctica con funcionalidades especiales añadidas que permitía publicar la información IoT generada al ecosistema de plataformas en el formato nativo de AIoTES (ontología AHA), así como recibirla. Se amplió el alineamiento para el DA de

Galicia para recibir esta información, ya que su modelo de datos original no incluía este tipo de información.

- MUVONE: este grupo mandó varios tipos de mensajes generados por su novedoso dispositivo IoT wearable (como brazalete) que permitía el control de la tensión, caídas, parámetros de medida del ejercicio físico medidos con un acelerómetro, enviando además información de posición GPS. Para su integración empleó una plataforma FIWARE, reusando el puente de FIWARE y creando un alineamiento para la publicación de esta información en AIoTES. No solamente se creó un alineamiento desde su data model a la ontología de ACTIVAGE sino también de la ontología al modelo de datos del DA de Grecia, de manera que se podía recibir los datos del servicio y gestionarlos en la plataforma IoT. La finalidad de esta solución AHA es la prevención inteligente de la osteoporosis.
- SmartFloor: este grupo integró una solución AHA para el control de caídas o distintos accidentes en el ecosistema de ACTIVAGE. Para ello integró su solución AHA con la plataforma universAAL del DA de Grecia y proporcionó un alineamiento para poder publicar la información generada en este servicio dentro del ecosistema interoperable de plataformas. Esta solución AHA estaba basada en un tipo de sensor especial, una baldosa de suelo inteligente que podía detectar la presencia o no de personas y distintas situaciones de accidente de manera inmediata y automática.

Estos grupos crearon puentes o alineamientos para la SIL que contribuyeron a la expansión del ecosistema de ACTIVAGE y a la habilitación de interoperabilidad entre más sistemas.

Otra tarea realizada en el marco fue la evaluación técnica de los desarrollos de los miembros de OpenCall y su integración con AIoTES, ya que se participó como evaluadora. También, en el marco de la interoperabilidad semántica se asesoró sobre el modelado de datos utilizando la ontología AHA de ACTIVAGE a distintos participantes.

6.5. Integración de la suite de interoperabilidad

Una vez finalizado el desarrollo de los componentes de la capa de servicio, y definidas las herramientas y protocolos de seguridad y privacidad a emplear, se llevó a cabo la creación de la suite AIoTES mediante la integración de sus distintos componentes en un framework unificado. La integración de AIoTES fue una tarea compleja que requería:

- La integración de sus distintos componentes en un framework unificado: la SIL, el módulo complementario y transversal de seguridad y las herramientas desarrolladas para la Capa de Servicios. Esta integración implicaba la implementación de mecanismos de seguridad del MSP en las herramientas, lo cual no resultó ser una tarea trivial en la mayoría de casos.
- Mecanismos de seguridad para el framework integrado, como conexión segura y autenticación, lo que implicó y gestionar la interacción con el gestor de identidades.
- La creación de un API para AIoTES que unificase las APIs de cada uno de los componentes y añadiese nuevas operaciones necesarias para el framework integrado, como métodos específicos para la gestión de tokens de seguridad.
- Proporcionar un despliegue instantáneo del framework y de los componentes seleccionados. Esto se consiguió aprovechando la virtualización de los componentes mediante Docker y Docker-Compose. Se utilizó la herramienta Portainer para la gestión gráfica y fácil del despliegue de un gran número de componentes virtualizados.
- La integración de una Interfaz Gráfica de Usuario para aportar gran usabilidad al despliegue y la configuración de componentes que se desearan utilizar. Se utilizó la Interfaz Gráfica proporcionada por la herramienta Portainer para tal fin.
- Finalmente, la virtualización completa del framework mediante tecnología Docker, Docker Compose y Docker Swarm.

Adicionalmente, fueron necesarias tareas de testeo. En primer lugar fue necesaria la verficación del correcto funcionamiento de los componentes a integrar siguiendo los pasos y tests proporcionados por los desarrolladores. En segundo, una vez se realizó la integración del framework, el testeo de los mecanismos de seguridad y el correcto funcionamiento del MSP, además de la comprobación del funcionamiento correcto de los componentes en el framework integrado (despliegue y gestión de la seguridad). Más allá del testeo de componentes separados o tras la integración del framework se realizaron acciones de validación del uso del framework que se describen en otra sección.

Tras el despliegue del framework virtualizado, se puede acceder a él a través de una pasarela-API que gestiona mecanismos de seguridad como uso de certificados, conexión segura, autenticación y gestión de tokens para el acceso a recursos según el marco OATH 2.0. A diferencia del uso de un gestor web general, la pasarela-API ofrece un único punto de acceso a AIoTES, proporcionando una mayor seguridad gracias a esta medida. Las distintas rutas web para el acceso a recursos son por tanto ramificaciones de este punto de acceso. También actúa en cooperación con el MSP para la autenticación y acceso al backend de acuerdo con el protocolo OATH 2.0. El framework AIoTES muestra en primer lugar un gestor de despliegue gráfico de componentes (la herramienta Portainer) cuya interfaz gráfica es muy usable. Permite el despliegue o repliegue de componentes y herramientas a voluntad del usuario, que selecciona los componentes a utilizar. Además de la SIL, el MSP y las distintas herramientas, uno de los elementos a desplegar es la API unificada, creada con una plantilla específica en la pasarela-API en combinación con una interfaz gráfica Swagger para APIs. Se contribuyó en la integración en la selección y estudio de la herramienta pasarela-API a utilizar, en la creación de scripts de seguridad para la integración de los componentes, en el soporte técnico a los integradores de herramientas y testeo de la integración efectiva de sus componentes y en la integración de la autenticación, uso de conexión segura, gestión de tokens y seguridad OATH 2.0 para acceso a backend de distintas herramientas, y el diseño de la estructura de operaciones y rutas de la API unificada.

La suite resultante presenta gran usabilidad y fácil y rápido despliegue. El coste de la primera instalación se estimó de alrededor de una hora siguiendo las instrucciones indicados en la documentación para este fin.

Se contribuyó en las distintas versiones de AIoTES. En concreto, se coordinó la integración de la versión Lanzamiento Oficial de AIoTES 2.0 (AIoTES Official Release [207]) que sustituyó a la versión anterior AIoTES 2.0 Candidate Release. La versión 2.0 Official Release fue la primera que presentó todos los bloques de AIoTES integrados (SIL, seguridad, herramientas de la capa de servicio), además de que sus componentes estaban correctamente verificados y validados y se habían aplicado corrección de errores y mejoras identificadas.

Se gestionó la integración de la versión AIoTES Official Release 2.1 [207], junto con CEA, que incluía el componente Gestor de KPIs, para la monitorización de la situación y la evolución de los DA. Se ofrecieron opciones de diseño inicial y final para permitir su integración.

El paso después de la integración, validación y corrección de errores o aplicación de medidas de mejora potenciales, una vez que el framework estaba finalizado, fue la liberación del código y su publicación como código abierto.

6.5.1. Creación del API unificado

La API de AIoTES expone un conjunto de operaciones REST para la gestión y explotación de toda la funcionalidad de del framework. Engloba y unifica todas las APIs individuales de los distintos componentes, además de añadir operaciones que permiten la gestión de la seguridad. Este componente trabaja conjuntamente con el MSP para permitir la autenticación, autorización y confidencialidad de los usuarios. La API de AIoTES hace uso de HTTPS con certificados válidos y requiere la autenticación del usuario.

En el marco de esta tesis doctoral se contribuyó a la creación del API de AIoTES mediante el estudio de las distintas opciones de pasarela-API (express y KONG), la creación de librerías de http posts para su uso, testeo y evaluación, y la definición de las operaciones y estructura de rutas [220]. Se decidió el uso de express como pasarela-API por sus ventajas frente a KONG. Las operaciones y estructura de rutas

fueron evolucionando hasta la versión final, añadiéndose nuevas funcionalidades. La pasarela-API no solo despliega la interfaz de la API

6.5.2. Desarrollo de scripts para la integración del MSP

Como ya se ha mencionado, fue necesaria la creación de scripts específicos para la gestión de mecanismos de seguridad y la integración final de componentes en AIoTES, para la cual era necesaria realizar una integración no trivial con la capa de seguridad . Estos scripts los pudieron emplear los miembros técnicos del consorcio para sus componentes como alternativa sencilla en términos de integración al uso de plugins OATH 2.0 de KeyCloack u otros posibles métodos.

6.5.3. Testeo del funcionamiento

Se realizó una validación y testeo de 3 fases:

- Verificación de Componentes: en primer lugar, se verificó la funcionalidad correcta de los componentes individuales antes de integrarlos al framework
- Validación del Framework Integrado: tras la integración de los componentes en un framework unificado, se validaron aspectos de AIoTES como suite integrada:
    - Módulo de Seguridad: su funcionalidad no podía ser testeada y evaluada sin
    - Despliegue y correcta visualización de componentes: esta parte
    - Interoperabilidad (Casos de Uso de Interoperabilidad) : como aspecto crítico del proyecto, la interoperabilidad fue validada a través de 5 tipos de casos de uso avanzados . A diferencia de la validación de seguridad y despliegue, en sí no se estaba testeando la correcta funcionalidad del framework integrado, sino la utilización y aplicación en caso de uso reales de la interoperabilidad semántica que la SIL proporciona.
- Validación de AIoTES en DAs: se realizaron cuestionarios en entrevistas guiadas a responsables de DAs sobre su uso de AIoTES y los elementos

utilizados y desplegados, que recogieron opiniones y valoraciones sobre la dificultad de uso general con rúbricas muy subjetivas.

La primera fase de testeo, la verificación de componentes fue necesaria para detectar errores antes de integrar los componentes en AIoTES. Dos partes de la validación del framework se corresponden al testeo de la integración de este, comprobando que los componentes se despliegan y visualizan correctamente y el MSP proporciona mecanismos de seguridad a la suite unificada según lo esperado. Estas fases de validación y testeo fueron necesarias para considerar el framework finalizado y proceder a su lanzamiento oficial y distribución en los DAs.

La validación de los casos de uso de interoperabilidad representa una validación técnica de casos de uso de la interoperabilidad semántica entre los DAs. Finalmente, por otra parte, la validación de AIoTES en los DA recogió cierta información sobre el uso de AIoTES en los DA.

Se contribuyó con el diseño de tests, testeo de determinados componentes y finalmente, generación de los resultados y reportes desde la suite de testeo Squash para la justificación técnica del proyecto. Se tuvo un papel muy relevante en la validación de Casos de Uso de Interoperabilidad, muy ligados al desarrollo y uso de alineamientos.

6.5.4. Liberación como Código Abierto

Tras el testeo del framework y su uso y validación en los DA se procedió a su publicación como código abierto, a disposición de cualquier interesado en su uso o extensión.

6.5.4.1 *Política de Licencias*

Para la liberación de los componentes como código abierto se contribuyó con el estudio y selección de licencias, y el desarrollo de la política de licenciación de ACTIVAGE que marcaba y proporcionaba las reglas e instrucciones bajo las cuales se debía publicar el código de cualquier producto del proyecto. Esta acción se llevó a cabo conjuntamente con el grupo Insight. Se seleccionó la licencia Apache 2.0 [204] debido a sus características, ya que permite la publicación de código abierto satisfaciendo todas las necesidades identificadas y abriendo la puerta a su uso

comercial en condiciones de reconocimiento de autoría y origen. También, de manera alternativa, se ofreció la opción de utilizar la licencia EUPL [221] para la publicación de productos software generados en el proyecto ACTIVAGE.

Además de definirse la licencia a utilizar se proporcionaban instrucciones claras paso a paso para desarrolladores no familiarizados con el proceso de publicación de código abierto.

6.5.4.2 *Proceso de Publicación de Código Abierto*

Se coordinó la publicación del código del framework en la organización AIoTES en GitHub [207]. Además de la política de licencia se realizó la catalogación de cada componente en esquemas de categorías, se diseñó una política de nombres para identificar correctamente los componentes y que constituye una buena práctica de desarrollador, y se efectuó la inclusión, gestión de usuarios y diseño de la estructura política de la organización en GitHub. Se guió a los desarrolladores de componentes para que identificaran las dependencias de su código, así como las restricciones generadas para el uso de licencias, para que finalmente crearan los archivos de licencia y publicaran el código en GitHub. Así mismo, se llevó a cabo la publicación del código propio, y la creación de espejos de los componentes ya publicados del proyecto INTER-IoT.

Desde de la organización AIoTES en GitHub donde se encuentra el código liberado es posible la solicitud de consultas a desarrolladores ante dudas o problemas encontrados. Aunque se ofreció esta opción a los miembros del consorcio para gestión de incidencias y soporte técnico, la vasta mayoría de consultas se siguió haciendo por métodos tradicionales (correo electrónico, chat y videollamadas) hasta el final del proyecto.

6.6. Integración de las plataformas IoT en el Ecosistema Interoperable

Para la habilitación de interoperabilidad semántica de la información entre las distintas plataformas IoT de DAs (además de distintos sistemas IoT adicionales) han sido necesarios los siguientes pasos:

1) Desarrollo en el caso de ser necesario de puentes de comunicación y adaptación de formato sintáctico para los distintos tipos de plataformas a integrar en el ecosistema interoperable. Determinados puentes fueron reusados desde el proyecto INTER-IoT. Es importante notar que en general un mismo puente fue usado por distintos DA que utilizaban un mismo tipo de plataforma (p.e. DAs gestionados cada uno por una instancia de plataforma universAAL). Este paso solo es necesario si no existiese un puente disponible para cada tipo específico de plataforma a integrar.
2) Definición de la ontología central del ecosistema y ontología intermedia de traducción tras la decisión de la estrategia de uso del IPSM. Se utilizó para tal fin la ontología AHA creada en el marco del proyecto, la cual extendía GoIoTP.
3) Identificación de las ontologías o modelos de datos de cada uno de los DA o sistemas IoT a integrar. Es importante notar que aunque hubiese distintas plataformas de un mismo tipo (p.e. FIWARE) cada una empleaba modelos de información diferentes. En ciertos casos hubo que realizar un trabajo de recopilación y abstracción de la información representada en mensajes obteniendo su modelo generando una pequeña ontología RDF. La mayoría de DAs no soportaban las anotaciones y representación semántica del modelo de datos, pero este problema pudo ser resuelto con el uso de la SIL y el formalismo IPSM-AF para la programación de los alineamientos.
4) Creación de los alineamientos semánticos necesarios para cada plataforma. En la Tabla 6.4 se vieron los alineamientos que se crearon en el proyecto para la integración de las distintas plataformas o sistemas.
5) Instalación del motor de interoperabilidad (SIL o AIoTES). Esta instalación se hizo en primer lugar con la SIL de inter-IoT directamente, y más adelante con el framework integrado AIoTES, una vez estuvo disponible. Desde el punto de vista de la habilitación y gestión de interoperabilidad es indistinta la instalación de la SIL o de AIoTES. La diferencia es que la instalación de la suite de AIoTES provee de herramientas que podrían ser interesantes para los gestores o desarrolladores de los DA (o de AIoTES), y aporta un mecanismo extra de seguridad de acceso (uso de tokens en seguridad OATH 2.0 a nivel de interfaz de usuario en el uso del API).

6) Instalación de puentes y alineamientos semánticos y configuración de la SIL. Conexión de la plataforma y comprobación básica de la su correcta integración.

Figura 6.5 DAs que conformaron el ecosistema interoperable final de plataformas AHA

Como se ha podido ver anteriormente en las Tablas 6.1 y 6.2, la inclusión de los DAs se llevó a cabo en 2 periodos. Primeramente se integraron los 9 DAs iniciales y en un periodo posterior (9 meses después) se integraron 3 nuevos DAs provenientes de la Segunda Convocatoria de Abierta de Colaboración del proyecto. Otros sistemas IoT procedentes de la Primera Convocatoria Abierta de Colaboración se integraron en un punto intermedio (5-6 meses después de la primera integración).

En el marco de esta tesis doctoral se ha contribuido muy activamente a esta integración, liderando la tarea de alineamientos semánticos, gestionando la creación de guías, proporcionando soporte técnico a los DAs, y diseñando un sistema de

información de soporte eficiente con retroalimentación sobre el que se actualizaban muy rápido las consultas, observaciones y nueva información a anotar. También se llegaron a liderar las tareas de instalación y uso de la SIL, creación de alineamientos y puentes, soporte técnico a DAs y miembros de las OCs e integración de DAs con AIoTES.

Esta integración dentro de la arquitectura de interoperabilidad permitió el establecimiento de la interoperabilidad semántica de la información entre las distintas plataformas, permitiendo con ello importantes posibilidades técnicas y grandes beneficios fruto de la interoperabilidad, que pueden verse en la sección de casos de uso de interoperabilidad y validación.

6.7. Validación de la Solución de Interoperabilidad

6.7.1. Validación Técnica de Casos de Uso de Interoperabilidad

Desde una perspectiva general, los beneficios de la habilitación de la interoperabilidad semántica entre las plataformas IoT para gestión AHA son la posibilidad de intercambio y comprensión de información entre ellas, lo que permite la gestión de sensores virtuales de otra plataforma y la reusabilidad de aplicaciones y servicios entre las distintas plataformas.

En el marco del proyecto se definieron 5 casos de uso de alto nivel de interoperabilidad, fruto de la habilitación de la interoperabilidad semántica. En esta sección se describen todos ellos, así como la validación técnica de un ejemplo de cada tipo realizada por desarrolladores técnicos. Estos casos de uso se emplearon en los DA con usuarios reales, aunque esta validación está realizada por personal técnico que no eran ancianos usuarios finales de los Hogares Inteligentes. Estos Casos de Uso de Interoperabilidad (CUI) son:

- CUI 1: Gestión de sensores virtuales en otra plataforma
- CUI 2: Uso de aplicaciones nativas de otra plataforma
- CUI 3: Combinación de servicios entre plataformas

- CUI 4: Aplicaciones multiplataforma (basadas en el modelo de datos y API de AIoTES)
- CUI 5: Aplicación de interoperabilidad conjunta del ecosistema (todas las plataformas integrantes)

La validación de estos casos de interoperabilidad es en sí una validación de la interoperabilidad semántica y de los alineamientos semánticos. Las validaciones de los CUI se recogieron con la plataforma Squash de testeo del proyecto, detallando el proceso de pasos previos y comprobación técnica.

CUI 1: Sensores Virtuales: sensores gestionados en múltiples plataformas

Este caso de uso permite que en un DA desplegado con una plataforma A se puedan utilizar y gestionar dispositivos físicos IoT gestionados por otra plataforma B. Para ello se crean réplicas "virtuales" de este sensor en la plataforma A, que recibe la información IoT que recoge este sensor en el formato de datos este gracias a la traducción sintáctica y semántica que realiza la SIL como elemento intermedio entre las dos plataformas. La información de este sensor podrá ser utilizada por las aplicaciones nativas de la plataforma A que requieren del uso de información en el modelo semántico y formato de datos de la plataforma A, esto es, como si fuera un sensor de la plataforma A.

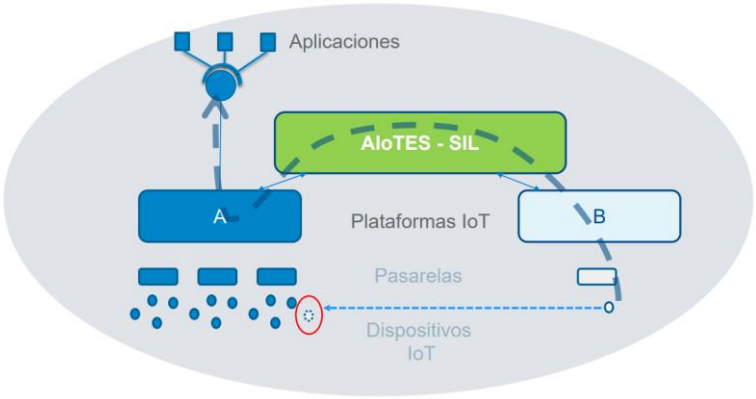


Figura 6.6 Caso de Uso de Interoperabilidad 1

Validación de CUI 1: Sensores de condición física de universAAL en la plataforma SOFIA2

Desde una plataforma universAAL (testbed o DA) se emplean distintos dispositivos médicos: una báscula, un tensiómetro, un coagulómetro y un pulsómetro. Se hicieron réplicas virtuales de estos sensores en la plataforma SOFIA2 del DA de Galicia. Se envió la información generada por los dispositivos a través de la SIL desde la plataforma universAAL empleando un alineamiento de traducción desde la ontología general de universAAL a la ontología AHA de ACTIVAGE. Después, automáticamente desde el API de la SIL se redireccionó a la plataforma SOFIA2 utilizando un alineamiento de traducción desde la ontología AHA al modelo de datos de SOFIA2. Mediante las asociaciones de identificador de dispositivo se asoció en SOFIA2 las medidas hechas por los dispositivos en la plataforma universAAL a los dispositivos virtuales ya creados. Desde el punto de aplicaciones nativas sobre SOFIA2, estos sensores eran indistinguibles de los sensores reales gestionados por SOFIA2, y su información se gestionaba de la misma manera en las aplicaciones. Estos sensores eran utilizados por el programa de monitorización doméstica remota AHA llamado TELEA del servicio autonómico gallego de salud. De esta manera, usuarios de la plataforma universAAL podían disfrutar de este servicio desde otros DAs [191]. Aunque las ontologías de cada DA con la plataforma universAAL tenían extensiones diferentes, estos mapeos eran comunes a todas.

Este caso de uso se validó en la Primera Revisión Técnica de proyecto llevada a cabo por la Comisión Europea. Se contribuyó con la creación de alineamientos, configuración de Inter-MW e IPSM de canales y en la creación de un script de gestión de datos y redirección en el flujo de ejecución realizado con NodeRED. Posteriormente se distribuyeron los alineamientos con los mapeos para universAAL para su reutilización en los DA gestionados por universAAL (Grecia, Madrid, Woquaz, Finlandia) interesados en el uso de servicios sobre la plataforma SOFIA2.

Además de este ejemplo, se validaron oficialmente muchos otros casos de sensores virtuales entre distintas plataformas de DAs, aunque solo era necesario proporcionar un único ejemplo por CUI para cubrir esta validación.

CUI 2: Uso de aplicaciones de terceros sobre una plataforma desde otra distinta

Desde un DA desplegado con una plataforma A, se pueden utilizar aplicaciones de terceros que se ejecutan sobre el API de la plataforma B. La respuesta de esta aplicación (datos resultado de su uso) pasa a través de la SIL hasta la plataforma A.

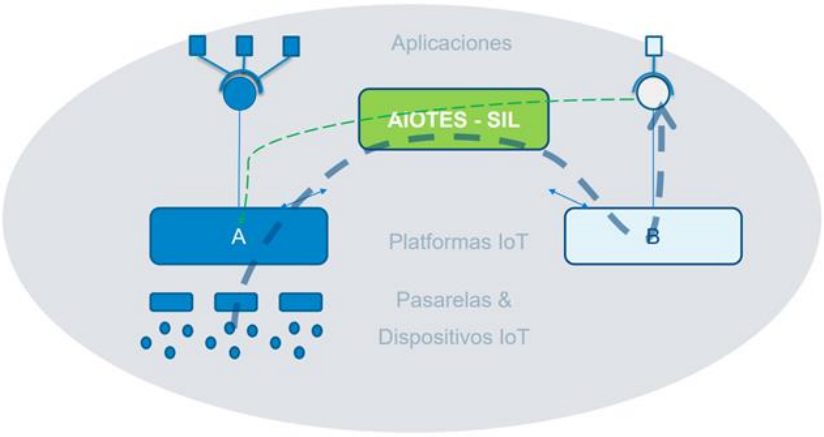


Figura 6.7 Caso de Uso de Interoperabilidad 2

Validación de CUI 2: Servicio de evaluación de pulsaciones o tensión

Desde el DA de Galicia se puede utilizar un servicio proporcionado por el DA de Grecia para la evaluación del nivel de pulsaciones o tensión, indicando información al respecto (p.e. si es un nivel correcto medio, alto, bajo, o en límites que podrían ser problemáticos, por lo que se aconseja pedir atención o consulta médica). Esto se hace mediante el envío, a través de la SIL, de información de pulsaciones o tensión a una aplicación en el DA de Grecia que evalúa esta información y devuelve su respuesta al DA de Galicia través de la SIL, con los identificadores de sensor y medida asociada. Se contribuyó al diseño de este caso de uso junto con Televes y CERTH, creando un análisis de flujo, modelando la respuesta en el modelo de datos de SOFIA2 y preparando los alineamientos necesarios para este intercambio de información y su configuración.

El uso de una aplicación de otra plataforma según la definición del CUI 2 no es en sí muy distinto a la del CUI 1 en cuanto a resultados o esfuerzo técnico, solo en la forma de envío y recepción de la información a y desde la aplicación, la cual es mucho más atípica. En el tiempo de vida del proyecto solo se generó un caso de interoperabilidad

de este tipo no por entrañar dificultades técnicas especiales o ser especialmente complejo, sino por lo atípico de esta forma de envío de información IoT. Para el uso de aplicaciones AHA nativas de otra plataforma IoT el enfoque más normal es utilizar un sensor virtual y visionar la respuesta directamente en la interfaz de la aplicación o servicio.

CUI 3: Sinergia entre aplicaciones de distintas plataformas

Mejorar aplicaciones existentes que se ejecutan sobre esta plataforma A con nuevas funciones proporcionadas desde otra plataforma B, desde una función proporcionada por su API o por una aplicación de esta plataforma B.

Esto implica una acción sinérgica a través de la SIL de una aplicación de una plataforma con otra aplicación o función de otra, refinando su funcionalidad. Esta acción sinérgica debe estar habilitada por medio de la interoperabilidad semántica entre plataformas y aplicaciones.

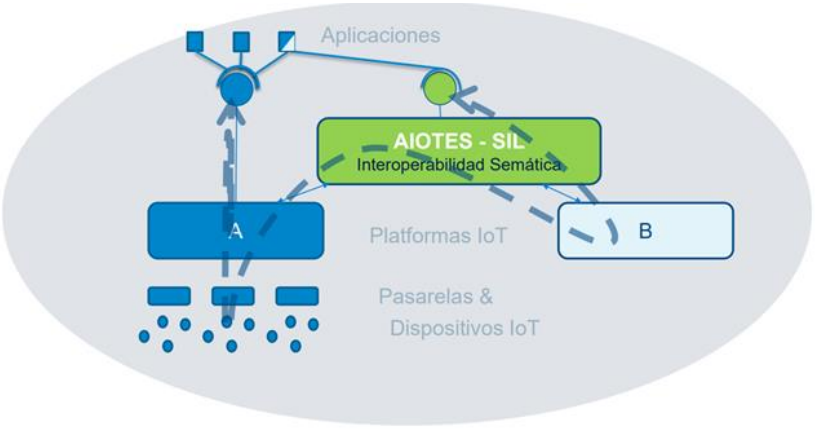


Figura 6.8 Caso de Uso de Interoperabilidad 3

Se validó como CUI 3, desde una interpretación muy laxa del concepto de aplicación, un intercambio de medidas de peso entre un testbed de FIWARE y el DA de Madrid, considerando una funcionalidad de universAAL para el registro de dispositivos como "aplicación". Sin embargo este caso claro de CUI 1 no encajaba perfectamente como CUI 3. En el marco de esta tesis doctoral se contribuyó en el desarrollo del testbed de

FIWARE, se crearon los alineamientos necesarios para incluir un sensor de báscula y se participó en el proceso de testeo.

Solo se dio un caso claro de combinación de aplicaciones para la mejora y refinamiento de una de ellas en el proyecto. Las medidas de tensión y pulsaciones pueden tienen picos instantáneos o espúreos debido a diferentes razones (imprecisiones del sistema de medida, movimientos bruscos al realizarlas, etc..). Es un caso general al utilizar un tensiómetro hasta que se estabiliza la medida. Estos picos no siempre son eliminados por tensiómetros IoT antes de enviar una medida, especialmente cuando se envía una secuencia de medidas continuas, y aunque solo en muy raras ocasiones con algunos instrumentos aparece un valor atípico y no representativo, puede ser conveniente efectuar un filtrado previo. Para ello se creó en el marco de esta tesis doctoral una aplicación para SOFIA2 (script de preprocesado) que podría ser utilizada por otros DAs. Se diseñó conjuntamente con Televés y CERTH. En concreto, el DA de Grecia tenía una aplicación de monitorización de condición vital en que se monitorizaba la evolución de estas medidas. Utilizando los alineamientos de subida de ambas plataformas, era posible enviar a través de la SIL medidas tomadas en el DA de Grecia (plataforma universAAL), filtradas en el DA de Galicia (plataforma SOFIA2) y reenviadas por la aplicación al DA de Grecia, como una medida de pulso o corazón normal en el caso de pasar el filtro. De ahí, se utilizaba en universAAL en la aplicación de monitorización. No era necesario realizar ningún tipo de extensión o cambio en los alineamientos de los DA, solo preparar la configuración de envío o suscripción a la información y un cambio sencillo indicando la fuente de alimentación de información IoT en la aplicación. Debido a que la inclusión de esta aplicación de filtrado sobre SOFIA2 (testeada en la zona de pruebas) fue duramente mucho tiempo estudiada en el DA, quedándose en espera, no fue validada en el periodo establecido para los CUIs.

CUI 4: Aplicaciones multiplataforma

Las aplicaciones que utilizan información IoT son típicamente específicas para una plataforma concreta. Las aplicaciones creadas sobre la API de AIoTES, con la que interactúan para conseguir información IoT, son en este sentido multiplataforma ya que se benefician de la homogeneización de la representación semántica de la información proveniente de las plataformas, utilizando la ontología AHA de ACTIVAGE

y un formato de datos común. Por tanto se pueden utilizar estas aplicaciones para una plataforma de DA u otra, independientemente de sus características, o inclusive para un conjunto de ellas simultáneamente. Este uso siempre tiene que darse desde la API de AIoTES o la API de la SIL.

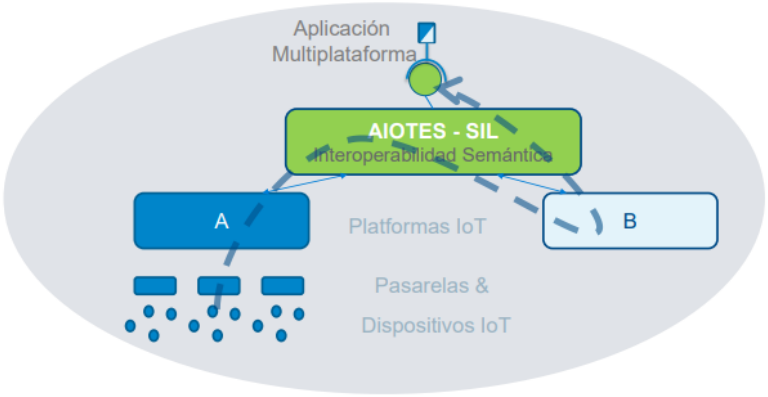


Figura 6.9 Caso de Uso de Interoperabilidad 4

Se crearón distintas aplicaciones multiplataforma en el proyecto. Se validaron ejemplos que cubrían este CUI 4, con el Gestor de datos de plataformas y con la aplicación SIL TOOL, creada en el marco de esta tesis doctoral. La SIL TOOL permite un uso multiplataforma y permite la explotación de la información IoT.

CUI 5: Interoperabilidad entre todo el ecosistema

Este caso de uso de interoperabilidad tiene como objetivo demostrar la interconexión e interoperablidad habilitada en todo el ecosistema de plataformas IoT a través de una aplicación que requiera obligatoriamente de la conexión y envío de datos de todas y cada una de las plataformas.

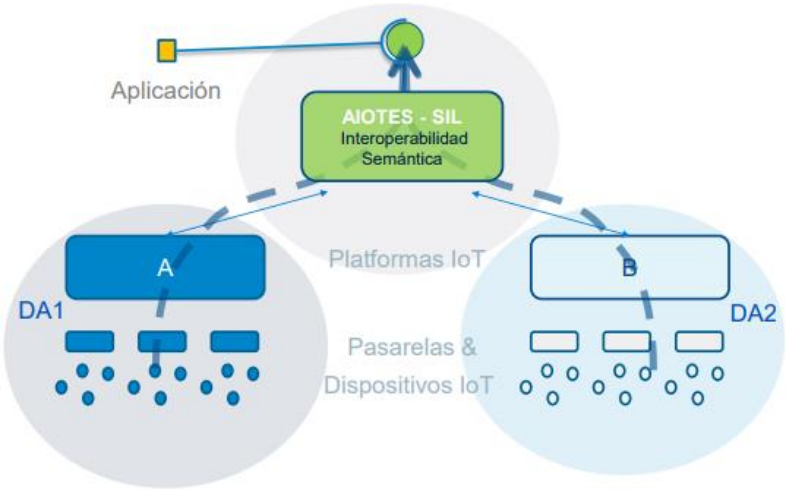


Figura 6.10 Caso de Uso de Interoperabilidad 5

En la validación oficial del proyecto se consideró que el Gestor de KPIs validaba el CUI 5 ya que representa la implementación de una aplicación común que recoge todos los valores de KPIs a nivel europeo procedentes de todas las plataformas de los 12 DSs de ACTIVAGE. Sin embargo, este no puede considerarse un caso de interoperabilidad semántica entre plataformas heterogéneas ya que es un sistema de recogida de KPIs basado en el uso de estándares y reglas comunes para el envío de información a una API manualmente desde cada DA, y no se corresponde al nivel de plataforma sino al de aplicación. Es en su lugar un caso de uso a nivel de aplicación de información no IoT (pero relacionada con los DAs) que obliga a usar un formato preestablecido de información. Por esta razón no se puede considerar en el marco de esta tesis doctoral un caso de uso fruto de la interoperabilidad semántica entre plataformas proporcionada por la SIL.

En este sentido, ejemplos de la conexión de múltiples DAs se vieron en las demostraciones técnicas del proyecto, aunque salvo una excepción no hay aplicaciones multiplataforma que validen y requieran la interconexión de todas y cada una de las plataformas (típicamente una aplicación de monitorización de ecosistema). Para una Revisión Técnica de Proyecto en el marco de esta tesis doctoral se desarrolló una aplicación web que permitía monitorizar visualmente de forma gráfica el envío de datos desde todas las plataformas a través de la SIL, e implicaba necesariamente

la conexión de todas las plataformas. Esta aplicación es ampliable para la inclusión de nuevos DA y solo requiere la configuración de la suscripción de información de las plataformas desde la SIL o desde AIoTES (o varias instancias de la SIL), realizable manualmente desde la API o de forma gráfica, rápida y sencilla con la SIL TOOL.

6.7.2. Validación en los DAs

Finalmente se realizó otra validación de AIoTES en los DA, informando sobre los usuarios reales finales involucrados. Esta se consideraba la última fase o nivel de validación, una vez testados los componentes, el framework integrado y validados técnicamente ejemplos de cada caso de interoperabilidad llevados a cabo en los DA.

Esta última fase de validación consistía en una serie de cuestionarios en entrevistas cortas guiadas sobre uso general de AIoTES realizadas a los responsables de los DA y gestores de plataforma, para recoger dos tipos de información:

- Usuarios finales de los DA beneficiados por el uso de un componente, bloque de componentes o elemento de AIoTES concreto.
- Opiniones y valoración sobre la dificultad subjetiva percibida respecto a un componente, bloque de componentes, elemento o caso de uso de interoperabilidad.

Esta validación no tenía como objetivo recoger el éxito de desarrollo, uso o despliegue del componente, o la utilidad de su aplicación y capacidad para cubrir las necesidades del DA, solo la dificultad subjetiva percibida y dar constancia de los usuarios finales relacionados con el uso de un componente. Para la valoración de dificultad se proporcionaba una rúbrica subjetiva del 0 al 10. No se especificaba claramente a que aspectos se refería la dificultad percibida, pero por extrapolación entendemos que a aspectos distintos en cada componente o elemento validados:

- -Desarrollo de alineamientos y desarrollo de puentes. Los DA no tenían que realizar el desarrollo de puentes pero se les pidió su opinión sobre este proceso, que en general valoraron que debía ser difícil.
- -Despliegue y posibilidad de uso sin especificar en que grado de los componentes que no eran la SIL (5 componentes o bloques de componentes)

la cual no aparece como componente en sí, sino como 7 elementos distintos que guardan relación con ella.

- -Creación de un caso de uso, sin especificar si se refiere a la creación de alineamientos, a la configuración de la SIL, si es la dificultad asociada en dar a acceso a una aplicación a compartir, o a otros aspectos que puedan estar relacionados con el caso de uso.

A diferencia de la validación de CUIs vista en el apartado anterior, esta parte no es una validación técnica, sino una encuesta de percepción subjetiva de dificultad respecto a un elemento. También, a diferencia de la validación técnica de CUIs, que solo pretendía mostrar un ejemplo de uso real por cada CUI a validar (aunque hubo DAs que voluntariamente añadieron más ejemplos testeados), en esta validación se buscaba en principio tener una visión global del uso de compontes o CUIs por parte de todos los DAs. Hay que notar que en las preguntas se reflejaba la presencia y número de usuarios finales reales beneficiándose de un componente o caso de uso. La valoración de dificultad percibida no provenía de la opinión o experiencia de estos, para los cuales el uso del framework era transparente, sino de los responsables del DA encuestados.

En la tabla de validación de los DA, se puede destacar que el componente que tuvo un mayor éxito y aceptación, a gran distancia de todos los demás, fue la SIL. Todos los DAs instalaron y desplegaron la SIL y se comprobó su funcionamiento. Todos los DAs desarrollaron alineamientos semánticos, el único esfuerzo de desarrollo que debían hacer los DA respecto AIoTES, el uso de cualquier otro componente solo implicaba simple despliegue automático. No solo se consiguió el uso básico de la SIL (publicación de información IoT a través de AIoTES traducida a la ontología de ACTIVAGE y posibilidad de recepción de información utilizando y ampliando en caso de ser necesario el alineamiento de bajada). También se desarrollaron muchos casos de interoperabilidad avanzados y complejos como los sensores virtuales y el uso de aplicaciones nativas de otra plataforma, y se cubrieron los CUIs.

El resto de componentes tuvo una implementación o despliegue por parte de los DA bastante moderada. Sin embargo, aunque no se refleje en la tabla hay que notar que el módulo de seguridad se utiliza obligatoriamente de manera transparente en cualquier instalación de AIoTES, así que se puede considerar que se utilizó en 12 DA.

Respecto al éxito y utilización, no hubo ninguna comprobación respecto al despliegue y correcto uso de los componentes, ni evidencia de ningún uso más allá de usuario básico o a un nivel avanzado desde la tarea de integración de AIoTES en DAs.

Tabla 6.5 Validación de AIoTES en DA: dificultad percibida de elemento de 0 a 10.

	CUI1	CUI2	CUI3	CUI 4	CUI 5 Gestor -KPIs	Puentes - Int. sintáctica	Alineamientos – Int. semántica	Data Lake federation	Seguridad	Marketplace	Data Analytics	Herraminetas Desarrollo	Deployment tools
DA-Galicia	4 4 4	6,5		N/A N/A	5	7,5	4		N/A			3,5	3,5
DA-Valencia			7		4	5	8,5	5		2			
DA Madrid			6,5		7	7,5	8	7,5	3	1		3	4
DA RER		4	7			9	8			1			
DA Grecia	8 8	8			5	9	10	8		2	5	6	6
DA Isère	9 6				2	6	9		3	1			
DA Woquaz	8 1,5		4		2	5	8			N/A	N/A	N/A	N/A
DA Leeds	N/A	3			N/A	7	8,5		N/A	N/A			
DA Finlandia	2		5,5		5	8	9	8					
Cataluña	6,5		4			7	8,5						
Sofia			6	9		3	6	6					
Lisboa			3	3,5		7	0						

Es importante notar que en general, el único desarrollo que era necesario para el uso del framework por parte de los DA era la creación de alineamientos semánticos, necesarios para poder beneficiarse de todas las ventajas aportadas por la interoperabilidad semántica. Todos los otros componentes solo implicaban un trabajo muy menor de despliegue, en la gran mayoría de casos incluido con el despliegue y configuración general de AIoTES, que se podía realizar en alrededor de una hora en la instalación inicial. Los puentes ya estaban disponibles con anterioridad, mediante reuso, actualización o inclusive desarrollo específico, pero sin recaer este trabajo sobre el DA. Por tanto, el único esfuerzo de desarrollo fueron los alineamientos, que fueron realizados en muchos casos por personas con pocos conocimientos semánticos. Esto se refleja en la nota de la dificultad subjetiva percibida, que contrasta con otras columnas ya que no se ha hecho distinción entre elementos de despliegue y uso y elementos de desarrollo.

Tabla 6.6 Usuarios finales de cada DA que se benefician del uso de la SIL

Despliegue AHA (DA)	Usuarios finales de los Hogares Inteligentes que se benefician del uso de la SIL
DA Galicia	708
DA Valencia	590
DA Madrid	508
DA RER (Región Emilia Romana)	0
DA Grecia	4
DA Isère	0
DA Woquaz	0
DA Leeds	550
DA Finlandia	60
DA Cataluña	60
DA Sofía	30
DA Lisboa	30

Hay que notar que cierta información sobre los casos de uso de la SIL parece haber estado indicada por los DA erróneamente probablemente por confusión entre un tipo de CUI y otro. Es notorio que el caso de interoperabilidad que no se hizo a través del IPSM o el desarrollo de alineamientos, sino mediante el simple envío de datos a una API (CUI5) fue muchísimo menos cubierto que los CUIs normales (CUI 1): solo 3 DA de 12 (25%) lo tenían listo al finalizar el tiempo de vida del proyecto, como quedó supervisado y documentado. Aún así, además de esos 3 DAs otros 5 valoraron que la dificultad que tuvieron para llevarlo a cabo fue relativamente baja, a pesar de que no llevaron a cabo esta integración.

También es notorio que los casos de uso 2 y 3 tienen múltiples DA que opinaron sobre su habilitación. Estos casos son muy raros no por tener distinta dificultad técnica sino por lo atípico de su uso, y solo se dio un caso de cada CUI en el ecosistema de DA (hay que notar que los DAs no estaban obligados a cubrir estos CUIs ni se les solicitó hacerlo, simplemente se hizo un recuento al final de los casos hechos). Todos los demás anotados no corresponden a CU2 o CU3. Desde el soporte técnico no se tuvo constancia de ningún intento de realización de estos, cuando en estos casos siempre se suele solicitar asesoría y una plantilla de inicio de alineamientos.

En el CUI 1 cabe destacar que, a pesar de ser intercambios entre 2 DAs generalmente, en muchos casos solo está marcado en un uno de los DA. Algún DA, como Madrid, no documentaron la realización de CUIs 1 cuando sí que está registrada la validación técnica de estos que se hizo en la fase anterior.

Sobre el CUI 4 solo implicaba utilizar alguna aplicación multiplataforma disponible en el proyecto, las cuales pueden utilizar información IoT de cualquier plataforma. Este era un caso de uso que requiere muy bajo esfuerzo por parte de un DA (despliegue y uso guiado). Por las respuestas dadas aparentemente solo 3 DAs aprovecharon estas aplicaciones a nivel de entorno real.

Respecto a la dificultad de uso de puentes es sorprendente la alta dificultad percibida por muchos DAs. Su instalación en la SIL es un proceso simple, rápido y bien documentado. La alta dificultad percibida se debe, aunque no esté reflejado en la tabla, a que el cuestionario preguntó por el desarrollo de puentes (que no era una tarea de los DA) y no por su instalación. Los DA valoraron que debía de ser un desarrollo difícil o de dificultad media, aunque no estaban familiarizados con él.

Hay que notar también que las evaluaciones sobre casos de uso avanzados o utilización avanzada del componente no se realizaron con ningún otro componente fuera de la SIL con los CUIs.

En conclusión, esta validación de AIoTES en los DA no es una validación y testeo hecho desde un punto técnico estrictamente hablando, sino un conjunto de opiniones y valoraciones de responsables de los DA hubiesen o no utilizado el componente o CUI. En cualquier caso demuestra que hubo usuarios del framework que dieron su opinión sobre el proceso de instalación y sobre su uso y deja constancia de que hubo usuarios finales beneficiados.

Se puede ver el número de usuarios que indirectamente se beneficiaba del uso de la SIL en cada DA según datos de los responsables y los gestores de plataforma de los DA en la Tabla 6.6 (debido a servicios potenciales habilitados). Dos DAs (Woquaz e Isère) debido a los estrictos protocolos y restricciones de seguridad por sus leyes locales, no les fue permitido el intercambio de datos a través de la SIL en entorno real, y otro no DA no llegó a habilitarlos fuera del entorno de pruebas (RER) en principio por problemas debidos al impacto COVID en su región y empresa con relación sanitaria. Los 9 DA restantes sí que habilitaron el uso de la SIL en entorno real, habiendo 2540 usuarios beneficiados.

A pesar de las observaciones hechas, de las posibles ambigüedades e imprecisiones a la hora de plantear, efectuar y responder a las preguntas, a la falta de una rúbrica con niveles bien definidos y a la falta de distinción entre desarrollo, despliegue y uso, la realización de estos cuestionarios y evaluaciones demuestra que hubo usuarios finales que se beneficiaron del uso de AIoTES y la interoperabilidad semántica entre plataformas, y gestores de DAs involucrados.

6.7.3. Validación por la Comisión Europea

El proyecto fue evaluado a nivel técnico por la Comisión Europea, realizándose distintas demostraciones técnicas y considerándose los objetivos técnicos de interoperabilidad entre clusters europeos de casas inteligentes satisfactoriamente conseguidos.

6.8. Ventajas del Framework de Interoperabilidad

Desde el punto de vista de la interoperabilidad entre plataformas, el uso del framework AIoTES no presenta ninguna ventaja añadida al uso de las herramientas Inter-MW o IPSM de forma independiente, o desde el framework de INTER-IoT. La interoperabilidad conseguida es equivalente y el motor de interoperabilidad es el mismo. Si bien el diseño de los mecanismos de seguridad son algo distintos en AIoTES y en INTER-FW, son prácticamente equivalentes en funcionalidad (autenticación, conexión segura, uso de tokens de seguridad, gestor de identidad).

La diferencia radica en el enfoque de la arquitectura de interoperabilidad de AIoTES, que fuera de un ámbito general entre las distintas capas de los sistemas IoT se centra solo en la interoperabilidad a nivel de plataforma (semántica y middleware) y se enfoca en ofrecer de manera adicional herramientas que podrían ser útiles a gestores de plataformas IoT o desarrolladores AHA.

Una pequeña diferencia respecto a escalabilidad es que AIoTES presenta limitaciones sobre la capacidad de inclusión de plataformas de la SIL debido a las restricciones de escalabilidad del módulo de seguridad. Por ello, potencialmente el uso del IPSM, o el IPSM en combinación con Inter-MW permite incluir a un número mayor de plataformas en un ecosistema interoperable. Sin embargo esto afecta solo a conjuntos con un número bastante elevado de plataformas.

Otras ventajas del framework AIoTES son:

- Virtualización: framework virtualizado que permite un despliegue instantáneo independientemente del sistema operativo en un entorno operacional aislado
- Instalación y despliegue de alrededor de una hora la primera vez
- Interfaz Gráfica de Usuario
- Código abierto

6.9. Conclusiones

En este capítulo, se ha descrito un caso de aplicación de la interoperabilidad semántica entre plataformas IoT heterogéneas a gran escala, con un gran número de plataformas y usuarios centrado en el área de AHA, donde IoT puede aportar soluciones a uno de los problemas críticos de la sociedad moderna: el envejecimiento incremental de la población y la atención especial que requiere.

Las herramientas utilizadas para la habilitación de la interoperabilidad semántica entre plataformas son el traductor semántico IPSM y el middleware de plataformas Inter-MW, ambos del proyecto INTER-IoT visto en el capítulo anterior. Estos dos elementos combinados pueden aportar tanto interoperabilidad sintáctica como semántica de manera automática una vez desplegadas las herramientas, preparada la conexión de sistemas a través de ellos, y desarrollado alineamientos semánticos de traducción y reusado o creado puentes de plataforma. Los puentes de plataforma son específicos para un tipo de plataforma concreta y pueden ser reutilizados para conectar a Inter-MW. Sin embargo un alineamiento es específico para la traducción unidireccional entre dos modelos semánticos de datos u ontologías, y cada instancia de plataforma tiene típicamente su modelo de información semántico propio, por lo que los alineamientos generalmente no se reutilizan. Por ello hace falta generalmente crearlos específicamente para cada instancia de plataforma a incluir en un ecosistema interoperable de plataformas mediante el uso del IPSM e Inter-MW.

Esta combinación de herramientas se ha denominado Capa de Interoperabilidad Semántica o SIL. En el proyecto ACTIVAGE forma parte de una suite para la interoperabilidad de plataformas IoT conformando un ecosistema interoperable (AIoTES). Esta suite define una arquitectura de interoperabilidad distinta a la definida por el conjunto de soluciones INTER-IoT ya que aunque comparte soluciones de interoperabilidad utiliza un enfoque distinto que comprende solo la interoperabilidad a nivel de plataforma (middleware y semántica) y pone una atención especial a la disponibilidad y uso de herramientas para desarrollar servicios AHA por lo que incluye una Capa de Servicios.

El framework AIoTES está compuesto por un motor de interoperabilidad semántica entre plataformas (SIL), una capa transversal de seguridad y una capa adicional de

servicios. Además, tiene un Marketplace desplegable asociado para la publicación o descarga de herramientas AHA y un Gestor de KPIs para la monitorización y gestión del ecosistema AHA interoperable. Este framework ofrece como ventajas para su uso la virtualización, una interfaz gráfica de usuario de alta usabilidad, una capa transversal de seguridad, y la capacidad para proporcionar interoperabilidad semántica entre plataformas IoT diferentes.

Mediante el uso de la SIL en AIoTES se ha podido proporcionar interoperabilidad semántica entre el conjunto de 12 plataformas de gestión de clústers de Hogares Inteligentes AHA o Despliegues AHA (DAs) en 12 ciudades y 9 países en Europa. Además, se han incluido otras plataformas o sistemas IoT a este ecosistema interoperable.

AIoTES se puede considerar un habilitador digital para la digitalización de Hogares de Población Envejecida y cuidado AAL y AHA, además de un habilitador de interoperabilidad entre plataformas.

A diferencia de los casos vistos en el capítulo anterior, este caso de uso de aplicación es a gran escala, tanto a nivel de número de plataformas (12 oficiales) como de usuarios finales (7100), en sistemas reales AHA. La solución técnica IPSM junto a Inter-MW queda validada con este caso de uso no solo a nivel de efectividad proporcionando interoperabilidad sintáctica y semántica y resolviendo la comunicación automática entre plataformas, sino también a nivel de escalabilidad y flexibilidad del ecosistema. El ecosistema AHA de ACTIVAGE tiene un gran número de plataformas IoT añadidas en diferentes periodos, lo que prueba también su escalabilidad y flexibilidad de evolución. Cabe destacar que estas soluciones de interoperabilidad no se habían validado a nivel de escalabilidad en otros casos de uso del proyecto INTER-IoT, y es con este caso de interoperabilidad a gran escala en un entorno AHA

Esta solución permite conseguir los objetivos de interoperabilidad inicialmente establecidos además de otros beneficios de la interoperabilidad semántica entre plataformas:

- La interoperabilidad semántica entre plataformas IoT inter e intra DA, entre los 12 DAs distintos

- El reuso, portabilidad o replicabilidad de aplicaciones entre plataformas de DAs
- La creación de un ecosistema interoperable AHA de plataformas IoT, creando un ecosistema inicial AHA europeo de gran número de usuarios
- La gestión de sensores en una plataforma ya gestionados por otra plataforma
- La creación de aplicaciones multiplataformas basadas en el modelo semántico de información de ACTIVAGE
- La habilitación de casos de interoperabilidad avanzados como la sinergia entre aplicaciones nativas de distinas plataformas

La solución de interoperabilidad para la creación del ecosistema de plataformas IoT con fines AHA se implementó de manera exitosa y fue validada técnicamente desde una perspectiva de interoperabilidad en múltiples casos de uso de los que se benefició un gran número de usuarios finales de los Hogares Inteligentes gestionados.

Esta solución combinada (SIL en AIoTES) podría utilizarse igualmente a la vista en el capítulo 5 (IPSM solo) para la creación de ecosistemas interoperables de plataformas heterogéneas en cualquier ámbito de uso, con la diferencia de que resuelve de una manera más sistemática la interoperabilidad sintáctica que el uso aislado del IPSM. Sin embargo, a pesar de que es posible su uso en cualquier ámbito de aplicación de plataformas IoT en que haya una necesidad de interoperabilidad, su arquitectura está específicamente diseñada para AHA, donde se podrían obtener mayores ventajas.

Capítulo 7
Conclusiones

"Esa semilla que podía parecer insignificante, contiene un árbol
que a su vez contiene un bosque"

Alejandro Jodorowsky

7.1. Conclusiones generales

Esta tesis doctoral se ha centrado en el estudio y la aplicación de habilitadores digitales para facilitar interoperabilidad a plataformas y sistemas IoT. En sí, se consideran habilitadores digitales todas las herramientas tecnológicas que ayudan o permiten llevar a cabo la transformación digital de nuestro mundo, y se puede notar en este sentido que dado que una de las mayores y más arduas barreras que dificultan esta transformación es la falta de interoperabilidad entre plataformas IoT, y que además, un requisito esencial para la digitalización es la existencia de conectividad y capacidad de comunicación (interoperabilidad técnica), las tecnologías que permitan el establecimiento de interoperabilidad son per se habilitadores digitales, al margen de sus otras funciones como puente entre el mundo físico y el digital.

Ha sido necesario el diseño, desarrollo e implementación de distintas herramientas tecnológicas o habilitadores digitales para lograr la interoperabilidad de sistemas IoT,

a diferentes grados (técnico, sintáctico y semántico) y en diferentes niveles de un sistema IoT. Este es un objetivo muy complejo debido a los diversos niveles que cubrir en las distintas capas o partes de un sistema IoT, las cuales tienen necesidades muy diferentes y requieren de soluciones muy distintas.

En particular, esta tesis se ha centrado especialmente en el mayor reto y preocupación sobre interoperabilidad IoT hasta el momento: la interoperabilidad semántica entre plataformas. También, dentro del ámbito de la interoperabilidad en la actual Internet de las Cosas se han visto habilitadores que permiten mejoras potenciales en cuanto a la maximización de la capacidad de las redes y determinados protocolos para proporcionar interoperabilidad técnica, una de las grandes preocupaciones de la Internet del Futuro. Y por otro lado, como otro de los niveles necesarios para poder conseguir la interoperabilidad semántica se han visto distintas formas de conseguir interoperabilidad sintáctica entre sistemas, es decir, comprensión del formato de datos en que se almacena la información, lo que permite que los datos que la representan puedan ser leídos.

En el recorrido visto de esta tesis doctoral se han conseguido todos los objetivos propuestos y se han documentado en esta memoria los resultados de esta investigación, procedimientos aplicados, y sus implicaciones en la situación actual del paradigma IoT.

Se ha investigado la situación actual de interoperabilidad en IoT, las causas que impiden o dificultan su habilitación, y las posibles soluciones para este problema de falta de interoperabilidad. Se ha explorado la creación de soluciones, mediante métodos conocidos como el alineamiento a estándares y habilitadores creados por iniciativas de integración IoT, mediante la refinación y mejora de la eficiencia de habilitadores de interoperabilidad técnica, y mediante nuevas estrategias y enfoques completamente innovadores que abarcan todos los tipos de interoperabilidad y a todos los niveles de sistemas IoT heterogéneos, incluyendo el nivel inter-plataforma. Por último se han diseñado, creado e implementado soluciones en estas líneas, y se ha evaluado cada una de ellas para poder validarlas. En conjunto, se consideran cubiertos todos los objetivos propuestos en el capítulo 1 con el fin de investigar causas y soluciones para la habilitación de la interoperabilidad y abrir el camino para la transformación digital sin las barreras y obstáculos causados por su carencia.

A continuación se resume brevemente los objetivos específicos alcanzados con los desarrollos de esta tesis, desglosados según se ha visto en los capítulos previos.

En concreto, en cuanto al análisis del estado del arte de la interoperabilidad en IoT, en el segundo capítulo se han identificado los problemas y la situación de la interoperabilidad en IoT, así como sus grandes ventajas y soluciones potenciales. Un análisis exhaustivo de la interoperabilidad en IoT ha permitido identificar tipos de soluciones potenciales al complejo problema de la interoperabilidad. Dos soluciones son las pasarelas inteligentes y las plataformas IoT, que permiten habilitar la interoperabilidad en las capas de dispositivo y gestión de la información IoT (middleware). Se han diferenciado dos estrategias para la interoperabilidad entre plataformas IoT:

- en primer lugar por alineación a estándares
- en segundo, se ha identificado otro tipo de enfoque ya utilizado por elementos como pasarelas: la adaptación o conversión de elementos, que en cierto modo ya se utiliza entre plataformas a nivel de middleware o aplicación mediante adaptaciones muy locales, limitadas y parciales ad hoc para solucionar un problema puntual, pero sin aportar ninguna solución reusable, genérica, sistemática y capaces de cubrir adaptaciones de modelos de información completos entre distintas plataformas.

En concreto, entre todos los desafíos respecto a la interoperabilidad en IoT, se ha identificado la inherente falta de interoperabilidad entre plataformas como uno de los retos más arduos pero más importantes a resolver, ya que la falta de comunicación entre ellas provoca la fragmentación del ecosistema global IoT

En el tercer capítulo, se ha visto como Multipath TCP, que es un habilitador de interoperabilidad técnica de por sí como protocolo de transporte, multiplica esta capacidad de TCP gracias a las grandes ventajas de la gestión multicamino y una gestión especial de la congestión y el tráfico. En esta línea, se ha abordado el reto del diseño, desarrollo e implementación de un algoritmo que permite multiplicar los beneficios del control de congestión MPTCP y ofrece únicas capacidades y ventajas para esta gestión de tráfico que no tiene ningún otro algoritmo actual, salvando además los inconvenientes de estos. Este algoritmo permite combinar los beneficios

un control de congestión muy avanzado y eficiente utilizando un análisis inteligente de tiempos y la compatibilidad para coexistir con tráfico de conexiones agresivas. Esto permite obtener las grandes ventajas en cuestión de CC de MPTCP, junto con las de los algoritmos de CC basado en análisis inteligente de tiempos sin su gran debilidad: la incapacidad de coexistir con el tráfico mayoritario en Internet. Por ello, se considera que se ha diseñado e implementado un algoritmo extremadamente eficiente y con ventajas críticas frente a todos los existentes para MPTCP. Se ha realizado una implementación del algoritmo en el kernel de un sistema operativo real, Linux, en un módulo de control de congestión pluggable. El análisis de los resultados de la simulación de escenarios de tráfico MPTCP utilizando este tipo de control de congestión en comparación con el algoritmo estándar para MPTCP, LIA, ha confirmado sus ventajas potenciales, no solo a nivel de control de congestión local, sino global a la hora de promover un reparto con mayor equidad los recursos de la red entre la conexión propia y otras conexiones dentro de un enlace. Se propone este algoritmo y su uso en MPTCP como una solución para el creciente problema de saturación de las redes debido al aumento exponencial de tráfico proveniente de dispositivos IoT, ya que permite maximizar la capacidad de habilitar interoperabilidad técnica de las redes y del protocolo de transporte TCP. También se propone para conseguir una gestión muy eficiente de recursos en la red, de manera global en ella y no solo local, para Internet del Futuro, donde se espera que cobre gran importancia MPTCP.

En los siguientes capítulos de la tesis se ha abordado la interoperabilidad entre sistemas y plataformas IoT heterogéneas a niveles superiores (sintáctico y semántico) bajo diferentes estrategias. Encontrar soluciones a este problema es posiblemente el desafío más importante en IoT en la actualidad, ya que limita la integración horizontal de sistemas y plataformas, es la raíz de la fragmentación de la información global en IoT y de la existencia de silos verticales.

En primer lugar se ha abordado la habilitación de interoperabilidad por el uso de estándares, para la creación de un sistema AAL para la gestión inteligente de residencias. Mediante el uso de estándares abiertos del Open Geospatial Consortium en el marco de la Web de Sensores (SWE) y un Servicio de Observación de Sensores alineado con ellos, se ha construido un sistema de gestión flexible y escalable capaz

de integrar horizontalmente todo tipo de sensores, solucionando el conocido y recurrente problema de interoperabilidad "vendor lock-in" en sistemas de gestión IoT propietarios. Por otro lado, el uso de estos estándares y especificaciones, y las estructuras sintácticas y semánticas que aportan, conjuntamente con la creación de un vocabulario común, permite la interoperabilidad de la información entre distintos sistemas de residencias, y favorece la compatibilidad con otros sistemas o aplicaciones basados en el marco SWE y los estándares del OGC.

Más allá de la interoperabilidad entre sistemas por el uso de estándares, hay un gran vacío en el estado del arte actual sobre soluciones de interoperabilidad para plataformas IoT heterogéneas, que no siguen estándares comunes y tienen modelos de información completamente diferentes y dispares. La interoperabilidad por el uso de estándares tiene importantes limitaciones en su ámbito de aplicación, y solo se puede aplicar a un subconjunto muy pequeño de sistemas. Las plataformas heterogéneas difícilmente pueden cambiar sus estándares, modelos de información y soporte de datos. Por ello hay una grandísima necesidad de otro tipo de solución.

En este sentido, se ha participado en la iniciativa del proyecto INTER-IoT para la construcción soluciones y herramientas de interoperabilidad dentro de un enfoque orientado a proporcionar soluciones adaptadoras, que se describe en el capítulo 5. Una de las herramientas desarrolladas sigue la novedosa estrategia de adaptar los modelos de información de la plataforma emisora a la receptora, cambiando la representación de la información pero no su significado. Esta revolucionaria solución de interoperabilidad semántica entre plataformas IoT heterogéneas es el único traductor semántico para IoT, que permite la interoperabilidad semántica universal entre cualquier conjunto de plataformas. Esta solución se ha aplicado a distintos casos de uso (en concreto a casos de e-Salud y de AHA con usuarios reales en el marco de esta tesis doctoral) y ha demostrado su efectividad proporcionando interoperabilidad semántica entre plataformas IoT heterogéneas mediante adaptación de los modelos semánticos de información. Ofrece la posibilidad de crear ecosistemas interoperables de plataformas, en los que se puede compartir información entre todas ellas e inclusive entre las aplicaciones por encima, en lugar de limitarse a una interoperabilidad uno-a-uno con restricciones en la información compartida. Este ecosistema de plataformas se puede crear sobre una instancia del IPSM, es flexible en

el sentido de que puede incluir o eliminar fácilmente plataformas o expandir el soporte de traducción, presenta buena escalabilidad escalabilidad mediante el uso de. Por tanto es adecuado para la creación de ecosistemas de plataformas crecientes, que podrían inclusive conectarse e interoperar entre sí conectando instancias del IPSM. Además, presenta buena escalabilidad y mediante la estrategia de doble traducción con una ontología central el esfuerzo de inclusión de nuevas plataformas es lineal e se puede considerar independiente del número de plataformas ya incluidas conformando el ecosistema. Por todas estas razones, se puede concluir:

- Que la solución de traducción semántica propuesta proporciona una solución efectiva, genérica y adaptable a cualquier par de plataformas y modelos de semánticos de información para la habilitación de la interoperabilidad semántica entre ellas. Por ello es capaz de ofrecer una solución genérica, sistemática, única y altamente novedosa al mayor problema de interoperabilidad actual: la interoperabilidad semántica de la información entre plataformas IoT heterogéneas. Este problema constituye una de las mayores barreras para la digitalización del mundo e impide la creación de un ecosistema de plataformas IoT global.
- Por las características siguientes es apta para la creación de sistemas cambiables y crecientes de plataformas: capacidad de extender esta interoperabilidad entre un conjunto de plataformas entre sí, flexibilidad a la hora de incluir nuevas plataformas o cambios en ellas o en los modelos de información, buena escalabilidad y coste similar de inclusión de plataformas, además de posibilidad de conexión entre ellas.
- Puede utilizarse para crear ecosistemas semánticamente interoperables de plataformas IoT independientemente del tipo de plataformas, los estándares semánticos, del dominio de aplicación y los casos de uso.
- El coste de inclusión de plataforma consistiría en la creación de dos alineamientos semánticos para una comunicación bidireccional con las otras plataformas, y conectar el flujo de información compartida de la plataforma (saliente y entrante) a la instancia del IPSM utilizando la sintaxis RDF, lo que puede implicar utilizar adaptadores sintácticos.

- Por tanto, ofrece la posibilidad de creación de ecosistemas interoperables de plataformas IoT escalables, flexibles y cambiables, junto con la posibilidad de interconexión entre estos ecosistemas proporciona una solución a la fragmentación vertical entre plataformas IoT y posbilita la creación de un ecosistema global IoT compuesto por plataformas en el que pueda fluir fácilmente la información compartida entre ellas, sin la limitación de falta de interoperabilidad semántica. Esto permitiría la creación del ecosistema global IoT sin las barreras de interoperabilidad de la información proporcionando una herramienta que puede solucionar su fragmentación y permitir la unión de silos verticales, uno de los grandes problemas actuales en IoT que obstaculiza la transformación digital.

Para poder conseguir la habilitación de interoperabilidad a todos los niveles, el traductor semántico necesita un adaptador sintáctico y resolver la gestión de comunicaciones entre plataformas. Entre las posibles soluciones, esto puede conseguirse con su uso combinado con otro elemento de interoperabilidad, un middleware para la interconexión de plataformas (Inter-MW) también del proyecto INTER-IoT. El uso combinado de las dos herramientas hace más sencilla la conexión entre plataformas y soluciona de forma automática (una vez instalado y configurado) los detalles y procesos de la comunicación entre plataformas, además de realizar adaptación sintáctica de formatos de datos y proporcionar interoperabilidad sintáctica entre plataformas.

En el marco de esta tesis doctoral se ha llevado a cabo la aplicación combinada de estos habilitadores (SIL), desarrollando e implementando alineamientos semánticos y puentes de comunicación entre plataformas necesarios. Su implementación se lleva a cabo en el marco de un caso de uso AHA a gran escala a lo largo de toda Europa, aportando interoperabilidad entre plataformas para la gestión de Hogares Inteligentes en 12 ciudades europeas, con miles de usuarios reales, y creando un ecosistema interoperable IoT que constituye el primer ecosistema de AHA europeo, validando esta solución técnica.

- Esta solución técnica queda validada con este caso de uso a gran escala, no solo a nivel de efectividad proporcionando interoperabilidad sintáctica y

semántica y resolviendo la comunicación automática entre plataformas, sino también a nivel de escalabilidad y flexibilidad del ecosistema. El ecosistema AHA de ACTIVAGE tiene un gran número de plataformas IoT añadidas en diferentes periodos, lo que prueba también su escalabilidad y flexibilidad de evolución.

- El coste de inclusión de plataforma seguiría siendo independiente del número de plataformas, pero puede requerir el desarrollo de un puente de comunicación para el tipo de plataforma a conectar. Estos puentes son reusables y están disponibles como código abierto. Solo en caso de no estar disponible el puente para el tipo de plataforma a conectar sería necesario hacer un esfuerzo de desarrollo. Sería necesaria la conexión de la plataforma a Inter-MW y realizar la configuración de inclusión (incluyendo instalación de puentes y alineamientos).
- Como coste base para la creación del ecosistema sería necesaria la instalación, y conexión entre una instancia de Inter-MW y el IPSM.
- Esta solución combinada podría utilizarse igualmente a la vista en el capítulo 5 (IPSM solo) para la creación de ecosistemas interoperables de plataformas, permitiendo la creación del ecosistema global IoT al proporcionar una solución potencial, escalable y reusable al problema de fragmentación de silos verticales de plataformas y sistemas IoT. Con la diferencia de que esta solución combinada ofrece facilidades para la gestión de la comunicación entre plataformas y adaptación sintáctica. Proporcionaría una solución automática y sistemática (una vez preparada la instancia de la SIL, los puentes y la configuración inicial) para proporcionar interoperabilidad sintáctica y solucionar la gestión de comunicación entre plataformas.
- Esta solución puede emplearse para cualquier tipo de plataformas heterogéneas IoT, sintaxis o formato de datos empleado para soportar la información, modelo semántico de información, caso de uso o dominio.

Esta solución, así como otras del conjunto de herramientas de Inter-IoT, abre horizontes nuevos en el universo actual de IoT, habilitando posibilidades no accesibles

anteriormente, y acercándonos más a la visión de futuro de la IoT, en la que todo estaría interconectado de manera transparente, automática y sin barreras. La interoperabilidad en IoT aporta múltiples beneficios que promueven y facilitan la digitalización de nuestro mundo. Al permitir o habilitarla, se consiguen muchas sinergias, borrar barreras para ecosistemas globales de IoT y facilitar de manera muy significativa la digitalización de nuestro mundo, cuya barrera más importante actualmente es la fragmentación de IoT y la imposibilidad de crear ecosistemas IoT globales entre silos verticales.

Hay que notar también que, por otro lado, la interoperabilidad de IoT también tiene una importancia significativa sobre otros grandes habilitadores digitales. Tiene una gran relevancia en el análisis de Big Data, y en el Edge y Cloud Computing y en consecuencia también en el análisis de Inteligencia Artificial como Machine Learning o Deep Learning, porque facilita muy significativamente el procesamiento de datos y permite una mejora potencial del valor de los datos. Lo cual tiene también un impacto significativo en la digitalización de nuestro mundo y sobre la aplicación y efectividad de los habilitadores digitales de la Industria 4.0.

7.2. Trabajo Futuro

El trabajo realizado en la investigación desarrollada en esta tesis doctoral abre numerosas líneas de estudio, aplicación y trabajo futuro.

En primer lugar, los resultados del desarrollo de un nuevo tipo de control de congestión de Multipath TCP abren enormes posibilidades en el control eficiente del tráfico de manera global en las redes, y en términos de explotación de la funcionalidad multicamino.

Se han previsto las siguientes líneas de investigación futura:

- El algoritmo desarrollado crea de por sí una nueva familia de control de congestión, de naturaleza diferente a las ya establecidas y que ofrece ventajas críticas novedosas que no pueden ofrecer las demás familias. Los mecanismos innovadores del algoritmo DAIMD podrían adaptarse para utilizarse con otros mecanismos de control de congestión que ofrecen

ventajas concretas frente a Reno, añadiendo nuevos algoritmos en esta nueva familia de control de congestión (CC Híbrido). Algoritmos candidatos podrían ser CUBIC o BIC, que solucionan algunos fallos de diseño de Reno. La idea de diseño base sería efectuar una doble adaptación: (a) la adaptación del esquema de algoritmos de CC para TCP basados en pérdidas para proporcionarles un mecanismo eficaz de sensibilidad a la congestión y actuación eficiente frente a ella (b) la conversión de este esquema del algoritmo a un esquema MPTCP, añadiendo nuevos algoritmos a los pocos existentes para esta extensión de TCP, y ofreciendo nuevas opciones de control de congestión.

- La adaptación de los mecanismos de CC desarrollados sobre algoritmos MPTCP como BALIA y OLIA podrían aunar sus ventajas frente a LIA junto con las propias del mecanismo DAIMD (muy alta sensibilidad junto con compatibilidad para funcionar con el tráfico de Internet). De esta manera se podrían crear algoritmos DAIMD BALIA y DAIMD OLIA, que además de poder tener presumiblemente un mejor comportamiento en la gestión de cambios de camino que LIA podrían ofrecer también un control de flujo de transmisión y congestión muy avanzado.
- El uso del mecanismo Compound en algoritmos basados en pérdidas para MPTCP para transmisiones masivas de datos, combinado con algunos aspectos de DAIMD, podría ofrecer ventajas de ajuste inteligente de la congestión sin perder completamente la capacidad de transmisión ante otro tráfico competitivo en red. De esta manera se crearía otro algoritmo híbrido para MPTCP con funcionamiento interno diferente a DAIMD y orientado a un tipo de tráfico específico –para el que está especificamente diseñado Compound.
- La inclusión del algoritmo DAIMD como un módulo de control de congestión en el kernel de Android (sistema operativo basado en Linux en las capas base). De esta manera se podría ofrecer este sistema operativo para móviles con funcionalidad MPTCP y el control de congestión innovador de DAIMD. Esto posibilitaría su utilización en móviles, los cuales superan

abrumadoramente a los ordenadores en número en la Internet actual y tienen un gran protagonismo en IoT. Esta implementación podría permitir su uso y aceptación masiva por usuarios de móviles.

- Se considera estudiar su aplicación directa con tipos de tráfico de MPTCP, con especial atención a los generados por pasarelas inteligentes y tráfico IoT de redes de sensores. Esto permitiría estudiar y analizar en detalle las ventajas de su uso, posibilidades de explotación y aplicación, y mejoras potenciales del control de congestión para este tipo de tráfico y del uso eficiente de redes.
- Sería especialmente relevante el estudio del efecto del control de congestión y reparto de recurso en redes, para lo que se podría hacer uso de simuladores de redes y pruebas en redes reales. En especial sería muy interesante ver su aplicación y utilización en redes virtuales bajo el paradigma SDN y con transmisiones de datos masivas en 5G. Este mismo estudio también sería ampliable con algoritmos nuevos de esta familia. De esta manera se obtendría más información sobre potencial para poder solucionar el problema del tráfico creciente en redes y mejorar la capacidad de habilitar interoperabilidad técnica de las redes y del protocolo TCP.
- En una línea parecida, pero bajo el enfoque de sobrecarga y saturación de redes reales, un estudio sobre su potencial para aliviar situaciones de sobrecarga en la red y maximizar la capacidad de proporcionar interoperabilidad técnica de estas y del protocolo TCP. Este análisis será llevado a cabo utilizando simuladores de redes (incluyendo redes de nueva generación de alta capacidad como 5G). De este estudio se podrán derivar previsiblemente observaciones para posibles mejoras, la comparación de uso de MPTCP con distintos algoritmos con TCP y otros protocolos. Este estudio es de gran importancia para determinar su capacidad para aportar soluciones al problema del tráfico creciente de manera exponencial en redes, permitiendo optimizar el uso de la redes.
- También una línea de trabajo futura sería el estudio y explotación del potencial de MPTCP sobre el ahorro de energía. Al optimizar la capacidad

disponible, el uso de DAIMD o de algoritmos derivados puede contribuir a un menor coste energético de las transmisiones, una de las grandes preocupaciones en el uso de 5G en dispositivos portables como móviles. Este mismo trabajo también sería extensible a 6G.

- Por otro lado, MPTCP tiene aplicaciones interesantes en el ámbito de las comunicaciones secretas (el uso de varios caminos ofrece una gran protección a la captura de la información por terceros) y el uso de mecanismos como DAIMD permitiría mejorar la velocidad y efectividad de la transmisión haciendo estas comunicaciones más difíciles de interceptar. Este aspecto recoge un especial interés en el ámbito militar, especialmente en las situaciones de uso de canales de comunicación con anchos de banda residuales, bastante frecuentes en despliegues militares en zonas de conectividad muy limitada. No solo las comunicaciones estarían más protegidas, sino que tendrían la ventaja de poder utilizar canales de ancho de banda residual e ir añadiendo más o eliminando caminos desaparecidos según sea su disponibilidad cambiante. Esto permitiría aprovechar mucho mejor la poca conectividad disponible y evitar perder la conexión al desaparecer un camino. Por supuesto, la mejora de la eficiencia de las transmisiones y la regulación inteligente de la tasa de transmisión según el ancho de banda cambiante -ventajas del uso de MPTCP DAIMD- serían una ventaja crítica en estas situaciones.
- El estudio preliminar de su potencial sobre redes 6G, actualmente bajo especificación, que conformarán la Internet del Futuro y formarán parte de la Próxima Generación de IoT.

Respecto al trabajo realizado sobre la interoperabilidad de sistemas utilizando estándares de referencia, se preven distintas líneas futuras:

- En primer lugar, continuar el estudio que se hizo para mejorar el sistema SAFE-ECH y sus servicios incluyendo el uso de geolocalización dentro de edificios con novedosas técnicas como fingerprinting (utilizando información sobre la potencia de las redes locales, la localización de los puntos de

acceso). Esto permitiría poder utilizar la localización de elementos móviles y personas dentro del recinto de la residencia, cosa que actualmente es imposible con la tecnología GPS. Su aplicación se podría llevar en móviles (como en el estudio), además de incorporarse a otros dispositivos IoT como por ejemplo control de caídas (mejorando su alarma al poder enviar inmediatamente información crítica de posición sobre este accidente). Su uso en móviles o en pulseras inteligentes permitiría que de forma fácil pueda ser utilizado por cuidadores y residentes. Permitiría la mejora de muchos servicios y la creación de otros nuevos muy novedosos que ofrezcan una mejor calidad de servicio general de cuidado a los residentes.

- Así mismo, se podría ampliar el sistema para otros muchos casos de uso relevantes en residencias, mejorando los servicios ofrecidos o proporcionando otros para la mejora del bienestar de los residentes, los cuales serían fácilmente reproducibles en otras residencias que utilizasen este sistema. Esta línea se está tratando desde la empresa ISECO experta en gestión tecnológica de residencias.
- En una línea parecida, desde otra perspectiva, de ampliación del sistema, se podrían crear módulos de aplicaciones por encima de él que guardasen compatibilidad con otros sistemas basados en el SWE y sus estándares.
- Una aplicación de importancia notable sería la inclusión en el sistema o en aplicaciones por encima la explotación de los datos con el fin de poder hallar patrones e información oculta altamente valiosa, más allá del uso del CEP, mediante el análisis inteligente con técnicas de Inteligencia Artificial, Machine Learning y Deep Learning, aplicando por supuesto siempre alta privacidad sobre los datos. Esto podría proporcionar información altamente relevante oculta que ayudar y mejorar de forma muy relevante el sistema de gestión de residencias, lo que sería aplicable también a otros sistemas afines. Hay que tener en cuenta además, que su utilización en modo global en un conjunto de residencias permitiría la agregación de múltiples fuentes de información correladas, lo que permitiría un análisis más potente y de mayor

valor para proporcionar información valiosa para la mejora de la gestión y servicio en residencias.

- También se estudia exportar el sistema de gestión inteligente a otros ámbitos de aplicación como gestión de hospitales (o subsecciones de hospitales porque ya en ellas sería de gran utilidad potencial), gestión de centros de día y de Hogares Inteligentes especialmente diseñados para la tercera edad.
- Otras líneas de investigación futura sería su utilización en otros ámbitos de gestión inteligente IoT ya que potencialmente podría emplearse en cualquier área en que sea conveniente la monitorización inteligente de redes de sensores y actuadores, el control ambiental en entornos AMI o bien entornos sensorizables y la creación de servicios sobre información IoT.

Respecto a la utilización de las soluciones para la interoperabilidad semántica entre plataformas IoT heterogéneas, no alineadas por estándares comunes, mediante soluciones adaptadoras, las posibilidades de futura investigación, uso y explotación son inmensas. Proporcionan una solución al problema insalvable de la falta de interoperabilidad semántica entre plataformas IoT heterogéneas entre sí, el cual es el caso general, y lo ofrecen no solo entre dos concretas, sino potencialmente entre muchas a la vez, creando un ecosistema interoperable de plataformas altamente escalable con una sola instancia del IPSM (sola o conjuntamente con Inter-MW).

- La creación de nuevos puentes de comunicación de Inter-MW para la inclusión de nuevos tipos de plataformas, como zetta, Kaa o SENIORSOME. En especial se pretende el desarrollo de puentes para plataformas abiertas, y su publicación online, tanto a nivel de código compilado como código publicado bajo licencia Open Source, facilitando la utilización y el acceso a las soluciones de interoperabilidad entre plataformas de INTER-IoT.
- La creación de nuevos alineamientos para la inclusión de nuevas plataformas y sistemas IoT asociados gestionados por estas. En esta línea tiene especial interés su desarrollo para plataformas semánticas cuyo modelo de información está muy definido y basado en ontologías, como por ejemplo

OpenIoT, y puede ser reusable y extensible en las instancias de plataforma de este mismo tipo.

- La aplicación de las soluciones de Inter-IoT para la interoperabilidad semántica en múltiples ámbitos y dominios de aplicación (inclusive entre varios simultáneamente) en los que haya una necesidad de interoperabilidad y comunicación efectiva entre plataformas IoT. Dentro de estos ámbitos recibe un especial interés el área de la Ciudad Inteligente y la e-Salud, ya que en ellos la interoperabilidad entre múltiples sistemas es esencial e intrínsecamente necesaria y su habilitación en un grado muy alto o de manera completa proporciona enormes beneficios potenciales en comparación con soluciones parciales, y permitiría la coordinación entre sistemas y la creación de múltiples aplicaciones de interés fruto de esta interoperabilidad.
- Utilización de la solución de interoperabilidad semántica entre plataformas IoT en concreto en el área de la industria para ayudar a su transformación hacia la Industria 4.0. Sería especialmente interesante esta aplicación dado el gran potencial de la interoperabilidad en IoT de habilitar y potenciar los otros grandes habilitadores digitales (p.e. Computación en la Nube, Inteligencia Artificial). Este efecto sería aún mayor utilizando las nuevas generaciones de redes móviles 5G y 6G, donde la gran capacidad de conectividad permite una enorme explotación del paradigma IoT de forma imposible para redes anteriores como 4G. El uso de 5G permite una explotación masiva de en tiempo real de entornos altamente sensorizados, soportando sistemas complejos de IoT que efectúan transmisiones de información masivas. Esto permitiría el uso en la Industria 4.0. Abrir camino en la digitalización del mundo.
- Implementación de servicios IoT para el entorno portuario diseñados en el marco de esta tesis doctoral, los cuales serían posibles solo mediante a la interoperabilidad entre distintas plataformas IoT portuarias.
- En concreto, entre las herramientas desarrolladas, el traductor semántico del IPSM en sí podría ser ampliado incorporando nuevas funciones útiles para la

traducción una vez sean identificadas, y la inclusión de nuevas actualmente soportadas por el lenguaje SPARQL en la gestión de triples semánticos.

- También se podrían crear herramientas de testeo para traducción semántica rápidas y usables y un IDE para alineamientos, que de forma similar a por ejemplo Eclipse permitiera funciones de guiado y autocompletado, proporcionando una mayor facilidad y usabilidad a la habilitación de traducciones semánticas.
- El middleware Inter-MW podría ser mejorado agregando más funcionalidad para la sustitución de tablas de asignación entre elementos y preprocesado de mensajes, así como para la gestión de suscripciones de clústers de plataformas (sistemas-de-sistemas a sistemas-de-sistemas).
- Esta utilización y aplicación de las herramientas de interoperabilidad semántica entre plataformas podría hacerse dentro de otros proyectos de investigación, como ya sucede con H2020 PIXEL o LSP H2020 ACTIVAGE.
- Se podría estudiar la aplicación y beneficios en el mundo de la industria de este tipo de herramientas adaptadoras, facilitando el camino hacia la Industria 4.0. Fruto de la habilitación de interoperabilidad entre sistemas no inicialmente interoperables dentro de una fábrica o grupo de fábricas se podrían crear aplicaciones y servicios valiosos, fruto de la cooperación entre ellos o del intercambio de información relevante, aplicar análisis de Inteligencia Artificial con técnicas de Machine Learning o Deep Learning con datos enriquecidos de múltiples fuentes y con formato y modelo de información homogeneizado que proporcionen información muy valiosa, para lo que se puede utilizar Computación en la Nube o en la Pasarela.

Respecto AIoTES y su uso en grupos de Hogares Inteligentes para la tercera edad, se establecen futuras líneas de investigación:

- Mejora y evolución del framework AIoTES, añadiendo nueva funcionalidad y mejorando la actual, especialmente en el ámbito de privacidad, crítico para la gestión de datos AHA, estudiándose la posibilidad de utilizar el sistema

blockchain para seguridad y nuevos mecanismos para la gestión de la privacidad.

- Mejora de los servicios AHA ofrecidos en los Hogares Inteligentes y a través de las aplicaciones sobre las plataformas IoT que los gestionan, así como la inclusión de nuevos. Gracias a la interoperabilidad estos servicios podrían ser fácilmente compartidos o bien exportados a otras plataformas de gestión de Hogares Inteligentes de
- Mejora de los servicios AHA actuales mediante el uso de la interoperabilidad semántica, que permite compartir información valiosa entre sistemas y la creación de sinergias.
- Creación de nuevos servicios y aplicaciones fruto de la interoperabilidad entre sistemas y plataforma, aprovechando el valor añadido que aporta el intercambio de información valiosa y las posibilidades de cooperación, sinergia y coordinación entre sistemas.
- Creación de servicios multiplataforma utilizando las interfaces de comunicación de AIoTES y la ontología AHA de ACTIVAGE, siendo por tanto nativos de AIoTES. Estudio de su aplicación sobre múltiples plataformas AHA y grupos de usuarios de Hogares Inteligentes para la
- Inclusión de información y servicios de Ciudades Inteligentes, en los que se utilizan múltiples plataformas IoT que soportan sus servicios, mediante la incorporación estas en el conjunto interoperable de plataformas de gestión AHA conectadas a AIoTES.
- Inclusión de funcionalidad de consulta a registros médicos y servicios sanitarios, mediante la interoperación, garantizando al máximo la seguridad y privacidad de las consultas de datos.
- Integración de sistemas como residencias gestionadas por SAFE-ECH en el ecosistema de plataformas. Posible integración de la adaptación de SAFE-ECH para Hogares Inteligentes para ancianos y de la adaptación para Hospitales y Centros Médicos Inteligentes.
- Creación de un ecosistema europeo a gran escala de Hogares Inteligentes para la tercera edad, más allá de los pilotos del proyecto, incluyendo nuevos

sistemas y plataformas de gestión AHA. También con este fin se estudiará la creación de nuevos grupos de Hogares Inteligentes en otras regiones incluyendo novedosos avances tecnológicos en el ecosistema AHA. Este tema es especialmente importante en el futuro en términos de impacto social, ya que el envejecimiento de la población, su bienestar y los cuidados asociados que pueden necesitar es una preocupación crítica en la sociedad actual, que precisa de soporte tecnológico para dar apoyo y solucionar en la medida de lo posible este problema creciente.

Referencias

1. Noura M, Atiquzzaman M, Gaedke M. Interoperability in Internet of Things Infrastructure: Classification, Challenges, and Future Work. In: Lin Y-B, Deng D-J, You I, Lin C-C, editors. IoT as a Service. Cham: Springer International Publishing; 2018. p. 11–8. (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering).

2. Kshirsagar P, Pote A, Paliwal KK, Hendre V, Chippalkatti P, Dhabekar N. A Review on IOT Based Health Care Monitoring System. Lect Notes Electr Eng [Internet]. 2020 [citado 2021 Jul 28];570:95–100. Disponible en: https://link.springer.com/chapter/10.1007/978-981-13-8715-9_12

3. Lu Y. Industry 4.0: A survey on technologies, applications and open research issues. J Ind Inf Integr [Internet]. 2017 [citado 2020 Apr 22];6:1–10. Disponible en: https://linkinghub.elsevier.com/retrieve/pii/S2452414X17300043

4. Tao F, Qi Q, Wang L, Nee AYC. Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison. Engineering [Internet]. 2019 [citado 2020 Apr 22];5(4):653–61. Disponible en: https://linkinghub.elsevier.com/retrieve/pii/S209580991830612X

5. Noura M, Atiquzzaman M, Gaedke M. Interoperability in Internet of Things: Taxonomies and Open Challenges. Mob Networks Appl [Internet]. 2019 [citado 2021 Jul 28];24(3):796–809. Disponible en: https://doi.org/10.1007/s11036-018-1089-9

6. Gonzalez-Usach R, Yacchirema D, Julian M, Palau CE. Interoperability in IoT [Internet]. IGI; 2018 [citado 2021 Feb 18]. Disponible en: www.igi-global.com/chapter/interoperability-in-iot/224268

7. Gonzalez-Usach R, Yacchirema D, Julian M, Palau CE. Interoperability in IoT [Internet]. Handbook of Research on Big Data and the IoT. 2019 [citado 2021 Feb 18]. Disponible en: www.igi-global.com/chapter/interoperability-in-iot/224268

8. Fortino G, Savaglio C, Palau CE, de Puga J, Ghanza M, Paprzycki M, et al. Towards multi-layer interoperability of heterogeneous IoT platforms: The INTER-IoT approach. Internet of Things. 2018;0(9783319612997):199–232.

9. Ganzha M, Paprzycki M, Pawłowski W, Szmeja P, Wasielewska K. Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective. J Netw Comput Appl [Internet]. 2017 [citado 2018 Jul 2];81:111–24. Disponible en: http://linkinghub.elsevier.com/retrieve/pii/S1084804516301618

10. Lee SK, Bae M, Kim H. Future of IoT Networks: A Survey. Appl Sci [Internet]. 2017 [citado 2021 Jul 28];7(10):1072. Disponible en: https://www.mdpi.com/2076-3417/7/10/1072

11. Shafique K, Khawaja BA, Sabir F, Qazi S, Mustaqim M. Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. IEEE Access. 2020;8:23022–40.

12. Govindan K, Cheng TCE, Mishra N, Shukla N. Big data analytics and application for logistics and supply chain management. Transp Res Part E Logist Transp Rev [Internet]. 2018 [citado 2020 Apr 24];114:343–9. Disponible en: https://linkinghub.elsevier.com/retrieve/pii/S1366554518302606

13. Sarabia D, Gonzalez-Usach R, Palau CE. IoT Big Data Architectures, Approaches, and Challenges: A Fog-Cloud Approach. Res Anthol Archit Fram Integr Strateg Distrib Cloud Comput. 2021;227–50.

14. Zarabia D, Gonzalez-Usach R, Palau CE, Esteve M. Highly-efficient fog-based deep learning AAL fall detection system. Internet of Things [Internet]. 2020 [citado 2021 Jul 28];11:100185. Disponible en: https://linkinghub.elsevier.com/retrieve/pii/S2542660518300829

15. Xu L, Vrieze P De, Yu H, Phalp K, Bai Y. Interoperability of the future factory: an overview of concepts and research challenges. Int J Mechatronics Manuf Syst [Internet]. 2020 [citado 2021 Jul 28];13(1):3–27. Disponible en: https://www.inderscienceonline.com/doi/abs/10.1504/IJMMS.2020.108333

16. Cirillo F, Wu F-J, Solmaz G, Kovacs E. Embracing the Future Internet of Things. Sensors [Internet]. 2019 [citado 2021 Jul 28];19(2):351. Disponible en: https://www.mdpi.com/1424-8220/19/2/351

17. Vermesan O, Friess P, editors. Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds. Riverpublishers; 2016.

18. Pattar S, Buyya R, Venugopal KR, Iyengar SS, Patnaik LM. Searching for the IoT Resources: Fundamentals, Requirements, Comprehensive Review, and Future Directions. IEEE Commun Surv Tutorials. 2018;20(3):2101–32.

19. Vermesan O, Bacquet J. Next generation internet of things: distributed intelligence at the edge and human machine-to-machine cooperation. 2018.

20. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun Surv Tutorials. 2015 Oct;17(4):2347–76.

21. Paprzycki M. Keynote 5: Towards semantic interoperability in Internet of Things and beyond�. In: 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT). 2018. p. v--v.

22. Benson T, Grieve G. Why Interoperability Is Hard. In: Benson T, Grieve G, editors. Principles of Health Interoperability: FHIR, HL7 and SNOMED CT [Internet]. Cham: Springer International Publishing; 2021 [citado 2021 Jul 28]. p. 21–40. (Health Information Technology Standards). Disponible en: https://doi.org/10.1007/978-3-030-56883-2_2

23. Rahman T, Chakraborty SK. Provisioning Technical Interoperability within ZigBee and BLE in IoT Environment. In: 2018 2nd International Conference on Electronics, Materials Engineering Nano-Technology (IEMENTech). 2018. p. 1–4.

24. Farghaly K. Building Information Modelling and Asset Management: Semantic

and Syntactic Interoperability. Oxford Brookes University; 2020.

25. Ganzha M, Paprzycki M, Paw\textbackslashlowski W, Szmeja P, Wasielewska K. No Title. J Netw Comput Appl. :111–24.

26. Mckinsey Global Institute. The Internet of Things : Mapping the Value Beyond the Hype. 2015.

27. Kalamaras I, Kaklanis N, Votis K, Tzovaras D. Towards big data analytics in large-scale federations of semantically heterogeneous iot platforms. In: IFIP Advances in Information and Communication Technology. Springer New York LLC; 2018. p. 13–23.

28. Aloi G, Caliciuri G, Fortino G, Gravina R, Pace P, Russo W, et al. Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. J Netw Comput Appl [Internet]. 2017 [citado 2021 Feb 18];81:74–84. Disponible en: https://linkinghub.elsevier.com/retrieve/pii/S1084804516302405

29. A. Broring, A. Zappa, O.Vermesan, K. Främling, A. Zaslavsky, R. Gonzalez-Usach, P. Szmeja, C. Palau, M. Jacoby, I. P. Zarko, S. Sour- sos, C. Schmitt, M. Plociennik, S. Krco, S. Georgoulas, I. Larizgoitia, N. Gligoric, R. García-Castro, F. Serena, V. Orav. Advancing IoT Platform Interoperability. The Nederlands: River Publishers; 2018.

30. Chopra K, Gupta K, Lambora A. Future Internet: The Internet of Things-A Literature Review. In: 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon). 2019. p. 135–9.

31. Ganzha M, Paprzycki M, Pawlowski W, Szmeja P, Wasielewska K. Semantic technologies for the IoT - An Inter-IoT perspective. In: Proceedings - 2016 IEEE 1st International Conference on Internet-of-Things Design and Implementation, IoTDI 2016. Institute of Electrical and Electronics Engineers Inc.; 2016. p. 271–6.

32. Vivek S, Verma D, Krishnan P. Towards Solving the IoT Standards Gap. In: 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2018. p. 1441–7.

33. Ganzha M, Paprzycki M, Pawłowski W, Szmeja P, Wasielewska K. Towards

Semantic Interoperability Between Internet of Things Platforms. In: Gravina R, Palau CE, Manso M, Liotta A, Fortino G, editors. Integration, Interconnection, and Interoperability of IoT Systems [Internet]. Cham: Springer International Publishing; 2018 [citado 2018 Jul 2]. p. 103–27. Disponible en: http://link.springer.com/10.1007/978-3-319-61300-0_6

34. Ganzha M, Paprzycki M, Pawłowski W, Szmeja P, Wasielewska K, Palau CE. From implicit semantics towards ontologies — practical considerations from the INTER-IoT perspective. In: 2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC). 2017. p. 59–64.

35. Venceslau A, Andrade R, Vidal V, Nogueira T, Pequeno V. IoT Semantic Interoperability: A Systematic Mapping Study: In: Proceedings of the 21st International Conference on Enterprise Information Systems [Internet]. Heraklion, Crete, Greece: SCITEPRESS - Science and Technology Publications; 2019 [citado 2020 Jul 14]. p. 535–44. Disponible en: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0007732605350544

36. Jell T, Bröring A, Mitic J. BIG IoT – interconnecting IoT platforms from different domains. In: 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC). 2017. p. 86–8.

37. Žarko IP, Mueller S, Płociennik M, Rajtar T, Jacoby M, Pardi M, et al. The symbIoTe Solution for Semantic and Syntactic Interoperability of Cloud-based IoT Platforms. In: 2019 Global IoT Summit (GIoTS). 2019. p. 1–6.

38. Cimmino A, Oravec V, Serena F, Kostelnik P, Poveda-Villalón M, Tryferidis A, et al. VICINITY: IoT Semantic Interoperability Based on the Web of Things. In: 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS). 2019. p. 241–7.

39. Gonzalez-Usach R, Palau CE, Julian M, Belsa A, Llorente MA, Montesinos M, et al. Use cases, applications and implementation aspects for iot interoperability. Distrib Intell Edge Hum Mach Coop River Publ. 2018;139–73.

40. WSO2 Enterprise Service Bus as a Service Brings Agile Mediation to the Cloud

[Internet]. [citado 2021 Jul 27]. Disponible en: https://wso2.com/about/news/wso2-enterprise-service-bus-as-a-service-brings-agile-mediation-to-the-cloud/

41. Serrano M, Gyrard A, Tragos E, Nguyen H. FIESTAIoT Project: Federated Interoperable Semantic IoT/cloud Testbeds and Applications. In: Companion Proceedings of the The Web Conference 2018 [Internet]. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee; 2018 [citado 2021 Jul 27]. p. 425–6. (WWW '18). Disponible en: https://doi.org/10.1145/3184558.3186199

42. Soldatos J, Kefalakis N, Hauswirth M, Serrano M, Calbimonte J-P, Riahi M, et al. OpenIoT: Open Source Internet-of-Things in the Cloud. In: Podnar Žarko I, Pripužić K, Serrano M, editors. Interoperability and Open-Source Solutions for the Internet of Things. Cham: Springer International Publishing; 2015. p. 13–25. (Lecture Notes in Computer Science).

43. Rahman H, Hussain MI. A comprehensive survey on semantic interoperability for Internet of Things: State-of-the-art and research challenges. Trans Emerg Telecommun Technol [Internet]. 2020 [citado 2021 Jul 28];31(12):e3902. Disponible en: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3902

44. Ganzha M, Paprzycki M, Pawłowski W, Szmeja P, Wasielewska K. Towards Semantic Interoperability Between Internet of Things Platforms. In Springer, Cham; 2018 [citado 2018 Jul 2]. p. 103–27. Disponible en: http://link.springer.com/10.1007/978-3-319-61300-0_6

45. Inter-IoT Docs [Internet]. [citado 2021 Jul 28]. Disponible en: https://inter-iot.github.io/

46. Xu SS, Chen C, Chang T. Design of oneM2M-Based Fog Computing Architecture. IEEE Internet Things J. 2019;6(6):9464–74.

47. Kim J, Choi S-C, Yun J, Lee J-W. Towards the oneM2M standards for building IoT ecosystem: Analysis, implementation and lessons. Peer-to-Peer Netw Appl [Internet]. 2018 [citado 2020 Nov 27];11(1):139–51. Disponible en: http://link.springer.com/10.1007/s12083-016-0505-9

48. Wu C-W, Lin FJ, Wang C-H, Chang N. OneM2M-based IoT protocol integration. In: 2017 IEEE Conference on Standards for Communications and Networking (CSCN). 2017. p. 252–7.

49. IoTivity [Internet]. [citado 2021 Jul 27]. Disponible en: https://iotivity.org/

50. Bauer M, Bui N, Jardak C, Nettsträter A. The IoT ARM Reference Manual. In: Bassi A, Bauer M, Fiedler M, Kramp T, van Kranenburg R, Lange S, et al., editors. Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model [Internet]. Berlin, Heidelberg: Springer; 2013 [citado 2021 Jul 27]. p. 213–36. Disponible en: https://doi.org/10.1007/978-3-642-40403-0_9

51. ITU: Committed to connecting the world [Internet]. ITU. [citado 2021 Jul 28]. Disponible en: https://www.itu.int:443/en/Pages/default.aspx

52. ETSI - Welcome to the World of Standards! [Internet]. [citado 2021 Jul 28]. Disponible en: https://www.etsi.org/

53. IPSO Alliance [Internet]. [citado 2021 Jul 28]. Disponible en: https://www.linkedin.com/company/ipso-alliance

54. Guindon C. Eclipse Kura \textbar The Eclipse Foundation [Internet]. [citado 2021 Jul 27]. Disponible en: https://www.eclipse.org/kura/

55. IoT Framework for Interoperability in the oneM2M Architecture - ProQuest [Internet]. [citado 2021 Jul 27]. Disponible en: https://www.proquest.com/openview/808e93c80d32809588aad190f0ed1ac1/1/advanced

56. oneM2M Sets Standards For The Internet Of Things & M2M [Internet]. [citado 2021 Jul 27]. Disponible en: https://www.onem2m.org/

57. Guindon C. Mihini \textbar The Eclipse Foundation [Internet]. [citado 2021 Jul 27]. Disponible en: https://www.eclipse.org/proposals/technology.mihini/

58. Tecnología de la Pasarela Intel® para IoT [Internet]. Intel. [citado 2021 Jul 27]. Disponible en: https://www.intel.com/content/www/es/es/embedded/solutions/iot-gateway/training/iot-gateway-training-overview.html

59. AGILE IoT Community website – Adaptive Gateways for dIverse muLtiple Environments [Internet]. [citado 2021 Jul 27]. Disponible en: https://agile-iot.eu/

60. Fortino G, Parisi D, Pirrone V, Fatta G Di. BodyCloud: A SaaS approach for community Body Sensor Networks. Futur Gener Comput Syst [Internet]. 2014;35:62–79. Disponible en: https://doi.org/10.1016/j.future.2013.12.015

61. A. Hamza A, Abdel-Halim IT, Sobh MA, Bahaa-Eldin AM. A survey and taxonomy of program analysis for IoT platforms. Ain Shams Eng J [Internet]. 2021 May [citado 2021 Jul 28]; Disponible en: https://www.sciencedirect.com/science/article/pii/S209044792100201X

62. Salhofer P. Evaluating the FIWARE Platform. In 2018 [citado 2021 Jul 27]. Disponible en: http://hdl.handle.net/10125/50615

63. Ferro E, Girolami M, Salvi D, Mayer C, Gorman J, Grguric A, et al. The UniversAAL Platform for AAL (Ambient Assisted Living). J Intell Syst [Internet]. 2015 [citado 2021 Jul 27];24(3):301–19. Disponible en: https://www.degruyter.com/document/doi/10.1515/jisys-2014-0127/html

64. Patonico S, Nguyen T-L, Shabisha P, Braeken A, Steenhaut K. Toward the inclusion of end-to-end security in the OM2M platform. J Supercomput [Internet]. 2021 [citado 2021 Jul 27];77(4):4056–80. Disponible en: https://doi.org/10.1007/s11227-020-03415-7

65. Gürgen L, Munilla C, Druilhe R, Gandrille E, do Nascimento J. sensiNact IoT Platform as a Service. In: Seghrouchni AEF, Ishikawa F, Hérault L, Tokuda H, editors. Enablers for Smart Cities [Internet]. Hoboken, NJ, USA: John Wiley & Sons, Inc.; 2016 [citado 2020 Nov 27]. p. 127–47. Disponible en: http://doi.wiley.com/10.1002/9781119329954.ch6

66. Waspmote, la plataforma de sensores para desarrollar proyectos de IoT [Internet]. Libelium ES. [citado 2021 Jul 27]. Disponible en: https://www.libelium.com/es/productos-iot/waspmote/

67. Zatar IoT Platform [Internet]. [citado 2021 Jul 27]. Disponible en: https://www.d-synergy.com/zatar-iot-platform

68. Sofia2.10 [Internet]. [citado 2021 Jul 27]. Disponible en: https://sofia2.readthedocs.io/en/latest/

69. Ahamed J, Chishti MA. Semantic interoperability in the internet of things - state-of-the-art and prospects. Int J Innov Comput Appl [Internet]. 2021 [citado 2021 Jul 28];12(2–3):77–89. Disponible en: https://www.inderscienceonline.com/doi/abs/10.1504/IJICA.2021.113747

70. Gyrard A, Bonnet C, Boudaoud K. Domain knowledge Interoperability to build the Semantic Web of Things W3C Workshop on the Web of Things.

71. W3C. Semantic Sensor Network Ontology [Internet]. 2017. Disponible en: https://www.w3.org/TR/vocab-ssn/

72. Gyrard A, Datta SK, Bonnet C, Boudaoud K. Cross-Domain Internet of Things Application Development: M3 Framework and Evaluation. In: 2015 3rd International Conference on Future Internet of Things and Cloud. 2015. p. 9–16.

73. Ganzha M, Paprzycki M, Paw\textbackslashlowski W, Szmeja P, Wasielewska K. Towards common vocabulary for IoT ecosystems—preliminary considerations. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag; 2017. p. 35–45.

74. Compton M, Barnaghi P, Bermudez L, García-Castro R, Corcho O, Cox S, et al. The SSN ontology of the W3C semantic sensor network incubator group. Web Semant Sci Serv Agents World Wide Web. 2012 Dec;17:25–32.

75. Janowicz K, Haller A, Cox SJD, Le Phuoc D, Lefrançois M. SOSA: A lightweight ontology for sensors, observations, samples, and actuators. J Web Semant [Internet]. 2019 May [citado 2021 Jul 27];56:1–10. Disponible en: https://www.sciencedirect.com/science/article/pii/S1570826818300295

76. Gyrad. M3-Lite Ontology - Machine-to-Machine Measurement [Internet]. [citado 2021 Jul 27]. Disponible en: https://lov.linkeddata.es/dataset/lov/vocabs/m3lite

77. Gyrard A, Serrano M. A Unified Semantic Engine for Internet of Things and

Smart Cities: From Sensor Data to End-Users Applications. In: 2015 IEEE International Conference on Data Science and Data Intensive Systems. 2015. p. 718–25.

78. SAREF: the Smart Applications REFerence ontology [Internet]. [citado 2021 Jul 27]. Disponible en: https://saref.etsi.org/core/v3.1.1/

79. Generic Ontology for IoT Platforms [Internet]. [citado 2018 Jul 2]. Disponible en: https://docs.inter-iot.eu/ontology/

80. Singh R. Traffic engineering in planet-scale cloud networks. Dr Diss [Internet]. 2021; Disponible en: https://scholarworks.umass.edu/dissertations_2/2220

81. Muro F-JM, Skorin-Kapov N, Pavon-Marino P. Revisiting core traffic growth in the presence of expanding CDNs. Comput Networks [Internet]. 2019 May [citado 2021 Jul 27];154:1–11. Disponible en: https://www.sciencedirect.com/science/article/pii/S1389128618309423

82. Morley J, Widdicks K, Hazas M. Digitalisation, energy and data demand: The impact of Internet traffic on overall and peak electricity consumption. Energy Res Soc Sci [Internet]. 2018 [citado 2021 Jul 27];38:128–37. Disponible en: https://www.sciencedirect.com/science/article/pii/S2214629618301051

83. Mostarda L, Navarra A, Nobili F. Fast File Transfers from IoT Devices by Using Multiple Interfaces. Sensors [Internet]. 2021 [citado 2021 May 13];21(1):36. Disponible en: https://www.mdpi.com/1424-8220/21/1/36

84. Silva C, Ferlin-Reiter S, Alay O, Brunstrom A, Kimura B. IoT Traffic Offloading with MultiPath TCP. IEEE Commun Mag. 2021;

85. Saha SK, Kannan A, Lee G, Ravichandran N, Medhe PK, Merchant N, et al. Multipath TCP in Smartphones: Impact on Performance, Energy, and CPU Utilization. In: Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access [Internet]. New York, NY, USA: Association for Computing Machinery; 2017 [citado 2021 May 13]. p. 23–31. (MobiWac '17). Disponible en: https://doi.org/10.1145/3132062.3132066

86. Wu J, Tan R, Wang M. Energy-Efficient Multipath TCP for Quality-Guaranteed Video Over Heterogeneous Wireless Networks. IEEE Trans Multimed.

2019;21(6):1593–608.

87. Gonzalez-Usach R, Molla D, Palau C. High-Speed M2M Data Transmission with Embedded MPTCP on WebRTC. In Spain: UM Publishers; 2019.

88. Borman D, Braden B, Jacobson V, Scheffenegger R. TCP Extensions for High Performance [Internet]. 2014 [citado 2021 May 13]. Disponible en: https://www.rfc-editor.org/info/rfc7323

89. Tahaei H, Afifi F, Asemi A, Zaki F, Anuar NB. The rise of traffic classification in IoT networks: A survey. J Netw Comput Appl [Internet]. 2020 [citado 2021 Jul 28];154:102538. Disponible en: https://www.sciencedirect.com/science/article/pii/S1084804520300126

90. Ford A, Raiciu C, Handley M, Bonaventure O. TCP Extensions for Multipath Operation with Multiple Addresses [Internet]. 2013 [citado 2021 Jul 27]. Disponible en: https://www.rfc-editor.org/info/rfc6824

91. Khalili R, Gast N, Popovic M, Le Boudec J-Y. MPTCP Is Not Pareto-Optimal: Performance Issues and a Possible Solution. IEEE/ACM Trans Netw. 2013;21(5):1651–65.

92. Usach RG, Kühlewind M. Implementation and Evaluation of Coupled Congestion Control for Multipath TCP. In: Szabó R, Vidács A, editors. Information and Communication Technologies. Berlin, Heidelberg: Springer; 2012. p. 173–82. (Lecture Notes in Computer Science).

93. Mishra A, Sun X, Jain A, Pande S, Joshi R, Leong B. The Great Internet TCP Congestion Control Census. Proc ACM Meas Anal Comput Syst [Internet]. 2019 [citado 2021 Nov 12];3(3):1–24. Disponible en: https://dl.acm.org/doi/10.1145/3366693

94. Ford A, Raiciu C, Handley M, Bonaventure O. TCP Extensions for Multipath Operation with Multiple Addresses [Internet]. 2013 [citado 2021 May 13]. Disponible en: https://www.rfc-editor.org/info/rfc6824

95. Scharf M, Ford A. Multipath TCP (MPTCP) Application Interface Considerations [Internet]. 2013 [citado 2021 Jul 27]. Disponible en: https://www.rfc-editor.org/info/rfc6897

96. Ford A, Raiciu C, Handley M, Barre S, Iyengar J. Architectural Guidelines for Multipath TCP Development [Internet]. 2011 [citado 2021 Jul 27]. Disponible en: https://www.rfc-editor.org/info/rfc6182

97. Postel J. Transmission Control Protocol [Internet]. 1981 [citado 2021 May 13]. Disponible en: https://www.rfc-editor.org/info/rfc0793

98. Liu Y, Qin X, Zhu T, Chen X, Wei G. Improve MPTCP with SDN: From the perspective of resource pooling. J Netw Comput Appl [Internet]. 2019 [citado 2021 Jul 27];141:73–85. Disponible en: https://linkinghub.elsevier.com/retrieve/pii/S1084804519301912

99. Allman M, Paxson V, Blanton E. TCP Congestion Control [Internet]. 2009 [citado 2021 Jul 27]. Disponible en: https://www.rfc-editor.org/info/rfc5681

100. Chowdhury T, Alam MJ. Performance Evaluation of TCP Vegas over TCP Reno and TCP NewReno over TCP Reno. JOIV Int J Informatics Vis [Internet]. 2019 [citado 2021 Jul 27];3(3). Disponible en: http://joiv.org/index.php/joiv/article/view/270

101. Gonzalez-Usach R. Design of Delay-Based Congestion Control Algorithm for Multipath TCP. Stüttgart Universität; 2012.

102. draft-xu-mptcp-congestion-control-00 [Internet]. [citado 2021 Jul 27]. Disponible en: https://datatracker.ietf.org/doc/html/draft-xu-mptcp-congestion-control-00

103. Chaturvedi RK, Chand S. Optimal Load Balancing Linked Increased Algorithm for Multipath TCP. Wirel Pers Commun [Internet]. 2020 [citado 2021 Jul 27];111(3):1505–24. Disponible en: https://doi.org/10.1007/s11277-019-06934-6

104. Nguyen K, Kibria MG, Ishizu K, Kojima F. A Study on Performance Evaluation of Multipath TCP Implementations. In: Proceedings of the Eighth International Symposium on Information and Communication Technology [Internet]. New York, NY, USA: Association for Computing Machinery; 2017 [citado 2021 Jul 27]. p. 242–8. (SoICT 2017). Disponible en: https://doi.org/10.1145/3155133.3155195

105. Yu Cao, Mingwei Xu, Xiaoming Fu. Delay-based congestion control for multipath TCP. In: 2012 20th IEEE International Conference on Network Protocols (ICNP) [Internet]. Austin, TX, USA: IEEE; 2012 [citado 2021 Jul 27]. p. 1–10. Disponible en: http://ieeexplore.ieee.org/document/6459978/

106. Kato T, Haruyama S, Yamamoto R, Ohzahata S. mpCUBIC: A CUBIC-like Congestion Control Algorithm for Multipath TCP. In: Rocha Á, Adeli H, Reis LP, Costanzo S, Orovic I, Moreira F, editors. Trends and Innovations in Information Systems and Technologies. Cham: Springer International Publishing; 2020. p. 306–17. (Advances in Intelligent Systems and Computing).

107. Kuehlewind M, Gonzalez-Usach R. A Vegas-based Approach for MPTCP Congestion Control. In: IETF Vancouver 84. IETF; 2012.

108. Allman M, Paxson V, Blanton E. TCP Congestion Control [Internet]. 2009 [citado 2021 May 13]. Disponible en: https://www.rfc-editor.org/info/rfc5681

109. Bisoy SK, Pattnaik PK. Fairness between TCP Reno and TCP Vegas in wired and wireless network. Int J Comput Syst Eng [Internet]. 2017 [citado 2021 Jul 27];3(1–2):14–26. Disponible en: https://www.inderscienceonline.com/doi/abs/10.1504/IJCSYSE.2017.083137

110. Saedi T, El-Ocla H. TCP CERL+: revisiting TCP congestion control in wireless networks with random loss. Wirel Networks [Internet]. 2021 [citado 2021 Jul 27];27(1):423–40. Disponible en: https://doi.org/10.1007/s11276-020-02459-0

111. Kato T, Haruyama S, Yamamoto R, Ohzahata S. mpCUBIC: A CUBIC-like Congestion Control Algorithm for Multipath TCP. In 2020. p. 306–17.

112. Raiciu C, Handley M, Wischik D. Coupled Congestion Control for Multipath Transport Protocols [Internet]. 2011 [citado 2021 May 13]. Disponible en: https://www.rfc-editor.org/info/rfc6356

113. Gonzalez R, Pradilla J, Esteve M, Palau CE. Hybrid delay-based congestion control for multipath TCP. In: 2016 18th Mediterranean Electrotechnical Conference (MELECON). 2016. p. 1–6.

114. Pokhrel SR, Singh S. Compound TCP Performance for Industry 4.0 WiFi: A

Cognitive Federated Learning Approach. IEEE Trans Ind Informatics. 2021;17(3):2143–51.

115. Gonzalez R, Pradilla J, Esteve M, Palau CE. Hybrid delay-based congestion control for multipath TCP. In: 2016 18th Mediterranean Electrotechnical Conference (MELECON). 2016. p. 1–6.

116. Chaturvedi RK, Chand S. MPTCP Over Datacenter Networks. In: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). 2018. p. 894–8.

117. Karimah SA. Comparative Analysis of QoE Multipath TCP Congestion Control LIA, CUBIC, and WVEGAS on Video Streaming. Int J Inf Commun Technol [Internet]. 2021 [citado 2021 Jul 27];7(1):31–9. Disponible en: https://socj.telkomuniversity.ac.id/ojs/index.php/ijoict/article/view/534

118. Ganzha M, Paprzycki M, Pawłowski W, Szmeja P, Wasielewska K. Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective. J Netw Comput Appl [Internet]. 2017 [citado 2021 Feb 18];81:111–24. Disponible en: https://linkinghub.elsevier.com/retrieve/pii/S1084804516301618

119. Sensor Web Enablement DWG \textbar OGC [Internet]. [citado 2021 Jul 28]. Disponible en: https://www.ogc.org/projects/groups/sensorwebdwg

120. OGC. OpenGIS sensor observation service implementation specification. Open Geospatial Consortium (OGC); 2006. 116 p.

121. Alkhomsan MN, Hossain MA, Rahman SMM, Masud M. Situation Awareness in Ambient Assisted Living for Smart Healthcare. IEEE Access. 2017;5:20716–25.

122. Gonzalez-Usach R, Yacchirema D, Collado V, Palau C. AmI Open Source System for the Intelligent Control of Residences for the Elderly. In: Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. Springer Verlag; 2018. p. 46–52.

123. Gulati N, Kaur PD. FriendCare-AAL: a robust social IoT based alert generation system for ambient assisted living. J Ambient Intell Humaniz Comput [Internet]. 2021 [citado 2021 Jul 28]; Disponible en: https://doi.org/10.1007/s12652-021-

03236-3

124. WHO | What is Healthy Ageing? WHO. 2018;

125. Kim DS, Chung BJ, Chung YM. Analysis of AMI Communication Methods in Various Field Environments. Energies [Internet]. 2020 [citado 2021 Jul 28];13(19):5185. Disponible en: https://www.mdpi.com/1996-1073/13/19/5185

126. Al-alawi AI. WiFi Technology: Future Market Challenges and Opportunities.

127. Kanaris L, Kokkinis A, Liotta A, Stavrou S. Fusing Bluetooth Beacon Data with Wi-Fi Radiomaps for Improved Indoor Localization. Sensors [Internet]. 2017 [citado 2021 Feb 18];17(4):812. Disponible en: http://www.mdpi.com/1424-8220/17/4/812

128. Zigbee - Zigbee Alianza [Internet]. Zigbee Alliance. [citado 2021 Jul 27]. Disponible en: https://zigbeealliance.org/es/solución/Zigbee/

129. Hariharakrishnan J, N B. Adaptability Analysis of 6LoWPAN and RPL for Healthcare applications of Internet-of-Things. J ISMAC [Internet]. 2021 May [citado 2021 Jul 28];2(2):69–81. Disponible en: https://irojournals.com/iroismac/V3/I2/01.pdf

130. Wang M-H, Chen L-W, Chi P-W, Lei C-L. SDUDP: A Reliable UDP-Based Transmission Protocol Over SDN. IEEE Access. 2017;5:5904–16.

131. Homepage - LoRa Alliance® [Internet]. [citado 2021 Jul 27]. Disponible en: https://lora-alliance.org/

132. MQTT - The Standard for IoT Messaging [Internet]. [citado 2021 Jul 27]. Disponible en: https://mqtt.org/

133. Bröring A, Echterhoff J, Jirka S, Simonis I, Everding T, Stasch C, et al. New Generation Sensor Web Enablement. Sensors [Internet]. 2011 [citado 2021 Jul 28];11(3):2652–99. Disponible en: https://www.mdpi.com/1424-8220/11/3/2652

134. Jirka S, Stasch C, Broring A. OGC Best Practice for Sensor Web Enablement Lightweight SOS Profile for Stationary In-Situ Sensors. Version 1.0. [Internet].

2014 [citado 2021 Jul 28]. Disponible en: https://repository.oceanbestpractices.org/handle/11329/1093

135. Chung C-C, Huang C-Y, Guan C-R, Jian J-H. Applying OGC Sensor Web Enablement Standards to Develop a TDR Multi-Functional Measurement Model. Sensors [Internet]. 2019 [citado 2021 Jul 28];19(19):4070. Disponible en: https://www.mdpi.com/1424-8220/19/19/4070

136. Wayland M. OpenGIS Sensor Model Language (SensorML) implementation and specification. Open Geospatial Consortium (OGC); 2007. 1-180 OGC 07-00 p.

137. Pace P, Gravina R, Aloi G, Fortino G, Fides-Valero k, Ibanez-Sanchez G, et al. IoT platforms interoperability for active and assisted living healthcare services support. In: 2017 Global Internet of Things Summit (GIoTS). 2017. p. 1–6.

138. Truong H-L. Dynamic IoT data, protocol, and middleware interoperability with resource slice concepts and tools: tutorial. In: Proceedings of the 8th International Conference on the Internet of Things [Internet]. Santa Barbara California USA: ACM; 2018 [citado 2020 Nov 27]. p. 1–4. Disponible en: https://dl.acm.org/doi/10.1145/3277593.3277642

139. Ganzha M, Paprzycki M, Pawlowski W, Szmeja P, Wasielewska K. Alignment-based semantic translation of geospatial data. In: 2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall) [Internet]. Dehradun, India: IEEE; 2017 [citado 2021 Feb 18]. p. 1–8. Disponible en: http://ieeexplore.ieee.org/document/8344716/

140. Fortino G, Russo W, Savaglio C, Shen W, Zhou M. Agent-Oriented Cooperative Smart Objects: From IoT System Design to Implementation. IEEE Trans Syst Man, Cybern Syst [Internet]. 2018 [citado 2021 Feb 18];48(11):1939–56. Disponible en: https://ieeexplore.ieee.org/document/8241454/

141. Bermudez-Edo M, Elsaleh T, Barnaghi P, Taylor K. IoT-Lite: a lightweight semantic model for the internet of things and its use with dynamic semantics. Pers Ubiquitous Comput. 2017;21(3):475–87.

142. Aloi G, Caliciuri G, Fortino G, Gravina R, Pace P, Russo W, et al. Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. J

Netw Comput Appl. 2017 Mar 1;81:74–84.

143. Giménez P, Molína B, Palau CE, Esteve M. SWE Simulation and Testing for the IoT. In: 2013 IEEE International Conference on Systems, Man, and Cybernetics. 2013. p. 356–61.

144. Reed C, Botts M, Davidson J, Percivall G. Ogc® sensor web enablement:overview and high level achhitecture. In: 2007 IEEE Autotestcon. 2007. p. 372–80.

145. Fox S. Observations and Measurements - Part 1 - Observation schema. Open Geospatial Consortium (OGC); 2007. p. pen Geospatial Consortium (OGC), Wayland, MA, 2007.

146. Consortium OG. Observations and Measurements - Part 2 - Observation Schema. Open Geospatial Consortium (OGC); 2007. 1-85 OGC 07-0022rl p.

147. Boots M, A. R. OGC ® SensorML: Model and XML Encoding Standard. Open Geospatial Consortium (OGC); 2014.

148. Simonis, I. OpenGIS sensor alert service implementation specification. Wayland, MA; 2006.

149. Velayutham V, Chandrasekaran S, Mohan S. Web user interface based on OGC standards for sensor cloud using big data. Int J Commun Networks Distrib Syst [Internet]. 2018 [citado 2021 Jul 28];20(4):389–412. Disponible en: https://www.inderscienceonline.com/doi/abs/10.1504/IJCNDS.2018.092143

150. Henson CA, Pschorr JK, Sheth AP, Thirunarayan K. SemSOS: Semantic sensor Observation Service. In: 2009 International Symposium on Collaborative Technologies and Systems. 2009. p. 44–53.

151. Pradilla J, Esteve M, Palau C. SOSFul: Sensor Observation Service (SOS) for Internet of Things (IoT). IEEE Lat Am Trans. 2018;16(4):1276–83.

152. SOS - Standardized, web-based upload/download of sensor data and sensor metadata [Internet]. 52°North Spatial Information Research GmbH. [citado 2021 Jul 28]. Disponible en: https://52north.org/software/software-projects/sos/

153. 52 North [Internet]. 52°North Spatial Information Research GmbH. [citado 2021 Jul 28]. Disponible en: https://52north.org/

154. 52 North Community - Associated Labs [Internet]. 52°North Spatial Information Research GmbH. [citado 2021 Jul 28]. Disponible en: https://52north.org/research/associated-labs/

155. 52 North Community [Internet]. [citado 2021 Jul 28]. Disponible en: https://wiki.52north.org/

156. McFerren G, Hohls D, Fleming G, Sutton T. Evaluating Sensor Observation Service implementations. In: 2009 IEEE International Geoscience and Remote Sensing Symposium. 2009. p. V--363--V--366.

157. SOS Server \textemdash MapServer 7.6.4 documentation [Internet]. [citado 2021 Jul 28]. Disponible en: https://www.mapserver.org/ogc/sos_server.html

158. Gonzalez-Usach R, Collado V, Esteve M, Palau CE. AAL open source system for the monitoring and intelligent control of nursing homes. In: 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC). 2017. p. 84–9.

159. Palau) JVPC (supervisor: PCE. SOSLite: Soporte para Sistemas Ciber-Fasicos y Computacion en la Nube (PhD Thesis). [Spain]: UPV; 2016.

160. Pradilla J, Palau C, Esteve M. SOSLite: Lightweight Sensor Observation Service (SOS). IEEE Lat Am Trans. 2015;13(12):3758–64.

161. SAFE-ECH PROJECT | Foston Europe [Internet]. [citado 2021 Jul 28]. Disponible en: https://www.foston.eu/safe-ech-project/

162. Bousquet J, Kuh D, Bewick M, Standberg T, Farrell J, Pengelly R, et al. Operational definition of Active and Healthy Ageing (AHA): A conceptual framework. J Nutr Health Aging [Internet]. 2015 [citado 2018 Oct 21];19(9):955–60. Disponible en: http://link.springer.com/10.1007/s12603-015-0589-6

163. Rudnicka E, Napierała P, Podfigurna A, Męczekalski B, Smolarczyk R, Grymowicz M. The World Health Organization (WHO) approach to healthy ageing.

Maturitas. 2020 Sep 1;139:6–11.

164. Medrano-Gil AM, De Los Ríos Pérez S, Fico G, Colomer JBM, Sáncez GC, Cabrera-Umpierrez MF, et al. Definition of technological solutions based on the Internet of Things and Smart Cities paradigms for active and healthy ageing through cocreation. Wirel Commun Mob Comput. 2018;2018.

165. Yacchirema D, de Puga JS, Palau C, Esteve M. Fall detection system for elderly people using IoT and Big Data. Procedia Comput Sci [Internet]. 2018 May [citado 2021 Feb 18];130(C):603–10. Disponible en: https://doi.org/10.1016/j.procs.2018.04.110

166. Sun AY, Zhong Z, Jeong H, Yang Q. Building complex event processing capability for intelligent environmental monitoring. Environ Model Softw [Internet]. 2019 [citado 2021 Jul 28];116:1–6. Disponible en: https://www.sciencedirect.com/science/article/pii/S1364815218307242

167. Esper [Internet]. EsperTech. [citado 2021 Jul 28]. Disponible en: https://www.espertech.com/esper/

168. SAS Core 2.0 [Internet]. [citado 2021 Jul 28]. Disponible en: https://52north.org/maven/repo/snapshots/org/n52/swe/sas/sas-core/2.0-SNAPSHOT/

169. 52North/SES [Internet]. 52°North Spatial Information Research GmbH; 2019 [citado 2021 Jul 28]. Disponible en: https://github.com/52North/SES

170. Messaging that just works — RabbitMQ [Internet]. [citado 2021 Jul 28]. Disponible en: https://www.rabbitmq.com/

171. Consortium OG. OGC Abstract Specification Topic 20 10-004r3/ISO 19156:2010. ISO standards; 2010.

172. (OGC). O&M XML Codification. Open Geospatial Consortium (OGC); p. OGC-100025rl.

173. W3C. RDF 1.1 XML Syntax [Internet]. [citado 2018 Jul 30]. Disponible en: https://www.w3.org/TR/rdf-syntax-grammar/

174. Sporny M, Kellogg G, Lanthaler M. Json-Ld 1.0. A JSON based Ser Linked Data.

2013;(January):1–33.

175. Gonzalez-Usach R, Julian M, Esteve M, Palau CE. IoT Semantic Interoperability for Active and Healthy Ageing. In: Pandey R, Paprzycki M, Srivastava N, Bhalla S, Wasielewska-Michniewska K, editors. Semantic IoT: Theory and Applications: Interoperability, Provenance and Beyond [Internet]. Cham: Springer International Publishing; 2021 [citado 2021 Jul 28]. p. 323–46. (Studies in Computational Intelligence). Disponible en: https://doi.org/10.1007/978-3-030-64619-6_14

176. Group PGD. PostgreSQL [Internet]. PostgreSQL. 2021 [citado 2021 Jul 28]. Disponible en: https://www.postgresql.org/

177. PostGIS — Spatial and Geographic Objects for PostgreSQL [Internet]. [citado 2021 Jul 28]. Disponible en: https://postgis.net/

178. Alhomayani F, Mahoor MH. Deep learning methods for fingerprint-based indoor positioning: a review. J Locat Based Serv [Internet]. 2020 [citado 2021 Jul 28];14(3):129–200. Disponible en: https://doi.org/10.1080/17489725.2020.1817582

179. Hosseini KS, Azaddel MH, Nourian MA, Azirani AA. Improving Multi-floor WiFi-based Indoor positioning systems by Fingerprint grouping. In: 2021 5th International Conference on Internet of Things and Applications (IoT). 2021. p. 1–6.

180. Molina B, Olivares E, Palau CE, Esteve M. A MultimoSdal Fingerprint-Based Indoor Positioning System for Airports. IEEE Access [Internet]. 2018 [citado 2021 Feb 18];6:10092–106. Disponible en: http://ieeexplore.ieee.org/document/8270589/

181. Ventura B, Vianello A, Rossi M, Frisinghelli M, Monsorno R, Costa A, et al. In-situ data workflow using OGC Sensor Web Enablement (SWE) [Internet]. 2019 [citado 2021 Jul 28]. Disponible en: https://bia.unibz.it/discovery/fulldisplay/alma991005772181001241/39UBZ_INST:ResearchRepository

182. Truong H-L, Gao L, Hammerer M. Service architectures and dynamic solutions

for interoperability of IoT, network functions and cloud resources. In: Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings [Internet]. New York, NY, USA: Association for Computing Machinery; 2018 [citado 2020 Nov 27]. p. 1–4. (ECSA '18). Disponible en: https://doi.org/10.1145/3241403.3241407

183. GITHUB. INTER-IoT framework [Internet]. 2018. [citado 2020 Mar 21]. Disponible en: https://github.com/INTER-IoT

184. Cankar M, Olivares Gorriti E, Markovič M, Fuart F. Fog and Cloud in the Transportation, Marine and eHealth Domains. In: Heras DB, Bougé L, Mencagli G, Jeannot E, Sakellariou R, Badia RM, et al., editors. Euro-Par 2017: Parallel Processing Workshops [Internet]. Cham: Springer International Publishing; 2018 [citado 2021 Feb 18]. p. 292–303. Disponible en: http://link.springer.com/10.1007/978-3-319-75178-8_24

185. Koumaras V, Kapari M, Papaioannou A, Theodoropoulos G, Stergiou I, Sakkas C, et al. IoT Interoperability on Top of SDN/NFV-Enabled Networks [Internet]. Edge Computing and Computational Intelligence Paradigms for the IoT. 2019 [citado 2020 Nov 27]. Disponible en: www.igi-global.com/chapter/iot-interoperability-on-top-of-sdnnfv-enabled-networks/232005

186. Palade A, Cabrera C, Li F, White G, Razzaque MA, Clarke S. Middleware for internet of things: an evaluation in a small-scale IoT environment. J Reliab Intell Environ [Internet]. 2018 [citado 2021 Mar 26];4(1):3–23. Disponible en: https://doi.org/10.1007/s40860-018-0055-4

187. Razzaque MA, Milojevic-Jevric M, Palade A, Clarke S. Middleware for Internet of Things: A Survey. IEEE Internet Things J [Internet]. 2016 [citado 2020 Apr 22];3(1):70–95. Disponible en: http://ieeexplore.ieee.org/document/7322178/

188. Yacchirema, D., Gonzalez-Usach, R., Palau, C. EM. IoT Platform Interoperability applied to the domain of transport and logistics. In.

189. Belsa A, Sarabia-Jacome D, Palau CE, Esteve M. Flow-Based Programming Interoperability Solution for IoT Platform Applications. In: 2018 IEEE

International Conference on Cloud Engineering (IC2E) [Internet]. Orlando, FL: IEEE; 2018 [citado 2021 Feb 18]. p. 304–9. Disponible en: https://ieeexplore.ieee.org/document/8360346/

190. Node-RED [Internet]. [citado 2021 Jul 27]. Disponible en: https://nodered.org/

191. Gonzalez-Usach R, Julian M, Esteve M, Palau C. Federation of AAL amp; AHA systems through semantically interoperable framework. In: 2021 IEEE International Conference on Communications Workshops (ICC Workshops). 2021. p. 1–6.

192. __. D5.2. INTER-Meth: Full-fledged Methodology for IoT Platforms Integration. 2017.

193. Cookbook summary - INTER-IoT CookBook [Internet]. [citado 2021 Jul 28]. Disponible en: https://inter-iot.readthedocs.io/projects/inter-iot-cookbook/en/latest/

194. Lacalle I, Llorente MÁ, Palau CE. Towards Environmental Impact Reduction Leveraging IoT Infrastructures: The PIXEL Approach. In: Montella R, Ciaramella A, Fortino G, Guerrieri A, Liotta A, editors. Internet and Distributed Computing Systems [Internet]. Cham: Springer International Publishing; 2019 [citado 2020 Apr 23]. p. 33–45. Disponible en: http://link.springer.com/10.1007/978-3-030-34914-1_4

195. 5G-PPP. H2020 5GENESIS project [Internet]. 2020. Disponible en: https://5genesis.eu/

196. Gardikis G, Papadakis N, Perentos A, Fotiou M, Phinikarides A, Georgiades M, et al. The 5GENESIS testing facility as an enabler for integrated satellite/terrestrial 5G experimentation. In: 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW) [Internet]. Marrakech, Morocco: IEEE; 2019 [citado 2020 Nov 27]. p. 1–6. Disponible en: https://ieeexplore.ieee.org/document/8902802/

197. ACTIVAGE. ACTIVAGE project. 2018.

198. Gulino M, Maggi C, Costa A, Mortara M, Luca I De, Minutolo M, et al. MOBILE HEALTH: STUDIO PILOTA SUL “MONITORAGGIO DECENTRALIZZATO ED IN

MOBILITÀ DEGLI STILI DI VITA" NELL'AMBITO DEL PROGETTO EUROPEO "INTEROPERABILITÀ DI PIATTAFORME ETEROGENEE IoT-INTER-IoT." Soc SINU Acts Vol. 2016;8.

199. Pace P, Aloi G, Gravina R, Fortino G, Larini G, Gulino M. Towards interoperability of IoT-based health care platforms: the INTER-health use case. In: Proceedings of the 11th EAI International Conference on Body Area Networks. Brussels, BEL: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering); 2016. p. 12–8. (BodyNets '16).

200. FIWARE. Estándar NGSI V2 [Internet]. [citado 2021 Jul 28]. Disponible en: https://fw-wiki.smartaraucania.org/modelado-datos

201. NGSI V2 -FIWARE [Internet]. [citado 2021 Jul 28]. Disponible en: https://swagger.lab.fiware.org/

202. Foundation F. Modelado de Datos en FIWARE - Estándar NSGI v2 [Internet]. Disponible en: https://fw-wiki.smartaraucania.org/modelado-datos]

203. Ganzha M, Paprzycki M, Pawlowski W, Szmeja P, Wasielewska K. Semantic technologies for the IoT - An Inter-IoT perspective. In: Proceedings - 2016 IEEE 1st International Conference on Internet-of-Things Design and Implementation, IoTDI 2016. Institute of Electrical and Electronics Engineers Inc.; 2016. p. 271–6.

204. Apache License, Version 2.0 [Internet]. [citado 2021 Jul 28]. Disponible en: https://www.apache.org/licenses/LICENSE-2.0

205. Vermesan O, Bacquet J. Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution. 2017.

206. Szmeja P, Ganzha M, Paprzycki M, Pawłowski W, Wasielewska K. Declarative Ontology Alignment Format for Semantic Translation. In: 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU). 2018. p. 1–6.

207. AIoTES [Internet]. GitHub. [citado 2021 Jul 27]. Disponible en: https://github.com/AIoTES

208. Yacchirema D, Gonzalez-usach R, Esteve M. Interoperability of IoT Platforms applied to the transport and logistics domain. 2018;00(34):0–9.

209. INTER-IoT. INTER-IoT project. 2018.

210. OpenIoT – Open Source cloud solution for the Internet of Things [Internet]. [citado 2021 Jul 27]. Disponible en: http://www.openiot.eu/

211. MediaClinics – Wearable Health Applications [Internet]. [citado 2021 Jul 27]. Disponible en: https://www.mediaclinics.it/en/

212. ekenku [Internet]. [citado 2021 Jul 27]. Disponible en: https://www.ekenku.com/?lang=en

213. eKauri [Internet]. [citado 2021 Jul 27]. Disponible en: https://www.ekauri.com/?lang=en

214. openHAB [Internet]. [citado 2021 Jul 27]. Disponible en: https://www.openhab.org/

215. Keycloak [Internet]. [citado 2021 Jul 28]. Disponible en: https://www.keycloak.org/

216. Fotiou N, Pittaras I, Siris VA, Voulgaris S, Polyzos GC. OAuth 2.0 authorization using blockchain-based tokens. arXiv200110461 [cs] [Internet]. 2020 [citado 2021 Jul 28]; Disponible en: http://arxiv.org/abs/2001.10461

217. INTER-IoT CookBook - Inter-MW bridges [Internet]. [citado 2021 Jul 27]. Disponible en: https://inter-iot.readthedocs.io/projects/inter-iot-cookbook/en/latest/inter-layer/mw2mw/mw2mw-recipe1/

218. INTER-IoT Docs - Inter-MW [Internet]. [citado 2021 Jul 27]. Disponible en: https://inter-iot.readthedocs.io/projects/inter-iot-cookbook/en/latest/inter-layer/mw2mw/foreword/

219. INTER-IoT/intermw-bridge-example [Internet]. INTER-IoT; 2019 [citado 2021 Jul 27]. Disponible en: https://github.com/INTER-IoT/intermw-bridge-example

220. ACTIVAGE. D5.3 Intermediate Validation Results. 2019.

221. European Union Public Licence \textbar European Commission [Internet].

[citado 2021 Jul 28]. Disponible en: https://ec.europa.eu/info/european-union-public-licence_en