Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingeniería
y Sistemas de Telecomunicación

SISTEMA DE AYUDA A LA SELECCIÓN DE SOLUCIONES DE PROTECCIÓN DE DATOS PERSONALES, PARA LOS PRODUCTOS Y SERVICIOS EN "INTERNET DE LAS COSAS"

TESIS DOCTORAL

José Antonio Sánchez Alcón

Licenciado en Documentación

2015

Centro de Investigación en Tecnologías de Software y Sistemas Multimedia para la Sostenibilidad

Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación

SISTEMA DE AYUDA A LA SELECCIÓN DE SOLUCIONES DE PROTECCIÓN DE DATOS PERSONALES, PARA LOS PRODUCTOS Y SERVICIOS EN "INTERNET DE LAS COSAS"

TESIS DOCTORAL

José Antonio Sánchez Alcón

Licenciado en Documentación

Directores de la Tesis:

Prof. Dra. Lourdes López Santidrián

Prof. Dr. José Fernán Martínez Ortega

Universidad Politécnica de Madrid

2015

DOCTORADO EN INGENIERÍA DE SISTEMAS Y SERVICIOS ACCESIBLES PARA LA SOCIEDAD DE LA INFORMACIÓN

Tesis Doctoral		
Título	Sistema de ayuda a la selección de soluciones de protección de datos personales, para los productos y servicios en "Internet de las Cosas"	
Autor	José Antonio Sánchez Alcón	
Co-Directora	Lourdes López Santidrián	VºBº.
Co-Director	José Fernán Martínez Ortega	VºBº.
Tribunal		
Presidente	Dr. Juan Manuel Meneses Chaus	
Secretario	Dr. Juana Sendra Pons	
Vocal	Dr. Luis Panizo Alonso	
Vocal	Dr. Luis Hernández Encinas	
Vocal	Dr. Iván Marsá Maestre	
Suplente	Dr. Agustín Martín Muñoz	
Suplente	Dr. Carlos García Rubio	
Lugar y fecha de lectura	E.T.S.I. y sistemas de Telecomunicación (U.P.M.)	
Calificación		

El Presidente El secretario Los vocales

Tesis Doctoral para la obtención del título de Doctor

por la Universidad Politécnica de Madrid

2015

Índice

Índice vii

Índice de figuras xi

Índice de tablas xii

Índice de ecuaciones xiv

Resumen xvii

Summary xviii

1 Introducción 1

1.1. Motivación. 3

1.2. Objetivos 6

1.3. Estructura del documento 7

2 Estado del arte 9

2.1. Estado del arte de la privacidad en IoT 11

2.2. Estado del arte en el ámbito de negocio o promotor 13

2.3. El estado del arte en el ámbito legal 18

2.4. Estado del arte en el ámbito tecnológico 19

2.4.1. Esquemas de autenticación y de distribución de claves 23

2.4.2. Esquemas de distribución de claves en base a la estructura de red 24

2.4.3. Esquemas deterministas de distribución de claves 25

2.4.4. Esquemas probabilísticos de distribución de claves 25

2.4.5. Mecanismos de enrutamiento y agregación segura de datos 26

2.4.5.1. Mecanismos contra ataques de análisis de tráfico 27

2.4.5.2. Mecanismos de agregación segura de datos. 27

2.4.6. Mecanismos de localización segura 29

2.4.7. Sistemas de detección de intrusiones 29

2.4.8. Esquemas basados en confianza 30

2.4.9. Mecanismos y defensas contra algunos ataques 30

2.5. Conclusiones 33

2.5.1. Conclusiones del marco de negocio o promotor 33

2.5.2. Conclusiones del marco jurídico 34

2.5.3. Conclusiones del marco de las tecnologías 35

3 Sistema de protección de datos personales para Internet de las Cosas 37

3.1. Introducción al modelo 39

3.2. Descripción del modelo 41

3.2.1. Sistema experto de negocio (BES) 44

3.2.2. Sistema experto jurídico (LES) 47

3.2.3. Sistema experto tecnológico (TSES) 49

3.3. Visión conjunta del sistema 51

3.4. Extensión del sistema 54

3.5. Evaluación del rendimiento 56

3.5.1. Recolección de eventos 56

3.5.2. Indicadores clave del rendimiento 57

3.5.3. Sistema de alarmas 60

3.5.4. Ahorro de costes 63

3.6. Conclusiones 66

4 Validación del sistema 69

4.1. Entorno de validación del sistema. 71

4.2. Servicios llevables 71

4.2.1. Caso 1. Granja lechera 73

4.2.2. Caso 2. Caballos de carreras 73

4.2.3. Caso 3. Equipo de fútbol 73

4.2.4. Caso 4. Equipo de bomberos 74

4.2.5. Resultados generales 74

4.2.6. Desarrollo de caso. Equipo de bomberos 76

4.3. Servicios para red eléctrica inteligente 80

4.3.1. Ataques y objetivos vs contramedidas 82

4.3.2. Servicios y mecanismos de seguridad 86

5 Conclusiones y trabajos futuros 91

5.1. Mejoras proporcionadas por el sistema 93

5.2. Beneficios del sistema 94

5.3. Cumplimiento de los objetivos 95

5.4. Trabajos futuros 96

6 Referencias y tabla de acrónimos 99

6.1. Referencias bibliográficas 101

6.2. Tabla de enlaces. 125

6.3. Acrónimos. 131

Índice de figuras

Figura 1. Información involucrada en el sistema. 42

Figura 2. Sistema de protección de datos personales (PSPS-IOT). 43

Figura 3. Etapas del procesamiento 44

Figura 4. Cadena de selección de mecanismos de seguridad. 52

Figura 5. Información involucrada en el sistema. 53

Figura 6. Centro de Operación de Red (*NOC*) 54

Figura 7. Servicio conjunto. Servicios compuestos. 55

Figura 8. Sistema de evaluación del rendimiento. 63

Figura 9. Maqueta de diseño y pruebas. 72

Figura 10. Esquema del servicio. 77

Figura 11. Gasto de recursos. 80

Figura 12. Cadena de mediación. 81

Figura 13. Visión general de la operación del sistema. 81

Índice de tablas

Tabla. 1. Servicios de seguridad (ZigBee, 6LoWPAN and BT-LE). 22

Tabla. 2. Primera parte de la Matriz de Utilidad. 45

Tabla. 3. Segunda parte de la Matriz de Utilidad 47

Tabla. 4. Relación de imperativos de seguridad. 48

Tabla. 5. Relación los imperativos y los objetivos de los ataques. 49

Tabla. 6. Plantilla de evaluación de impacto. 50

Tabla. 7. Catálogo de ataques. 51

Tabla. 8. Detección de ataques 58

Tabla. 9. Categorización de los ataques. 59

Tabla. 10. Relación de imperativos de seguridad - servicios de seguridad. 74

Tabla. 11. Valores típico en función del tipo de dispositivo. 75

Tabla. 12. Relación entre mecanismos disponibles para las pruebas. 75

Tabla. 13. Matriz de Utilidad: Del Servicio y del tipo de Red. 77

Tabla. 14. Conjuntos de datos y definición de los dominios de confianza. 78

Tabla. 15. Imperativos legales in formato DPIA-T. 78

Tabla. 16. Asignación de mecanismos disponibles para las pruebas. 79

Tabla. 17. Servicios de seguridad vs ataque para una Smart Grid. 84

Tabla. 18. Mecanismos de Autenticidad. 86

Tabla. 19. Mecanismos de Autorización. 87

Tabla. 20. Mecanismos de Disponibilidad. 87

Tabla. 21. Mecanismos de Confidencialidad. 88

Tabla. 22. Mecanismos de Integridad. 88

Tabla. 23. Mecanismos de No-Repudio. 88

Tabla. 24. Enlaces a los documentos. 129

Tabla. 25. Acrónimos utilizados en el documento. 132

Índice de ecuaciones

(1) Ecuación del Indicador de disponibilidad.

(2) Vector de la distribución de usuarios en su tipología correspondiente.

(3) Matriz de asignación de servicios de seguridad y privacidad.

(4) Vector de servicios de seguridad y privacidad disponibles.

(5) Vector de servicios asignados a cada tipo de usuarios.

(6) Ecuación de asignación de servicios de seguridad y privacidad para cada tipo de usuario.

(7) Aplicación de la ecuación a un caso práctico.

Agradecimientos

Quisiera agradecer sinceramente el apoyo recibido por parte de los directores de esta tesis, así como su inestimable ayuda, igualmente quiero agradecer al Centro de Investigación CITSEM (Centro de Investigación en Tecnologías de Software y Sistemas Multimedia para la Sostenibilidad), y en particular al equipo GRYS (Grupo de Redes y Servicios de Nueva Generación), donde he desarrollado la tesis y he recibido todo el apoyo que he necesitado. Verdaderamente ha sido un placer compartir estos años con los componentes del grupo de investigación donde me he sentido realmente cómodo y donde he podido inspirarme con la profesionalidad de todos sus componentes.

Un agradecimiento a la labor de los revisores de las publicaciones y congresos, porque sus comentarios han sido como “chispas” que han prendido nuevas ideas y enfoques.

No quisiera dejar pasar la ocasión de agradecer a mi familia todo el apoyo recibido. Muchas gracias por todo.

Muchas gracias a todos.

“Todo avance significativo comienza a partir de una idea que le surge a alguien, pero su verdadera causa raíz y el verdadero mérito es el trabajo en equipo”. (Experiencia propia).

“Un equipo de trabajo formado por personas, podría verse como un entramado de expectativas y objetivos, entre los que también deben considerarse las expectativas y objetivos personales. Una adecuada gestión de estas expectativas y objetivos, convierte al equipo en una maquina imparable de alcanzar objetivos”. (Frase de mi amigo Eusebio, auditor europeo de Calidad y una de las mentes más claras y realistas que he conocido. Se lo llevó la primavera de 2015. Sin duda allá donde esté y capte alguna oportunidad de mejora o algún punto de no calidad, continuará realizando “proyectos de mejora” sostenibles).

Resumen

Los nuevos productos y servicios de “Internet de las Cosas” nos harán más eficientes, con una mayor capacidad de actuación y una mejor comprensión de nuestro entorno. Se desarrollarán nuevas ayudas técnicas que permitirán prolongar nuestra vida activa, y muchas ventajas que hoy día nos costaría imaginar. Sin embargo coexistiremos con una gran cantidad de dispositivos que recopilarán información sobre nuestra actividad, costumbres, preferencias, etc., que podrían amenazar nuestra privacidad. La desconfianza que estos riesgos podrían generar en las personas, actuaría como una barrera que podría dificultar el pleno desarrollo de esta nueva gama de productos y servicios.

Internet de las Cosas, alcanza su significado más representativo con las Ciudades Inteligentes (Smart Cities) que proporcionan las herramientas necesarias para mejorar la gestión de las ciudades modernas de una manera mucho más eficiente. Estas herramientas necesitan recolectar información de los ciudadanos abriendo la posibilidad de someterlos a un seguimiento. Así, las políticas de seguridad y privacidad deben desarrollarse para satisfacer y gestionar la heterogeneidad legislativa en torno a los servicios prestados y cumplir con las leyes del país en el que se proporcionan estos servicios.

El objetivo de esta tesis es aportar una posible solución para garantizar la seguridad y privacidad de los datos personales en Internet de las Cosas, mediante técnicas que resulten de la colaboración entre las áreas empresarial, legislativa y tecnológica para dar confianza a todos los actores involucrados y resolver la posible colisión de intereses entre ellos, y también debe ser capaz de gestionar la heterogeneidad legislativa.

Considerando que gran parte de estos servicios se canalizan a través de redes de sensores inalámbricos, y que estas redes tienen importantes limitaciones de recursos, se propone un sistema de gestión que además sea capaz de dar una cobertura de seguridad y privacidad justo a medida de las necesidades.

Summary

New products and services offered by the “Internet of Things” will make people more efficient and more able to understand the environment and take better decisions. New assistive technologies will allow people to extend their working years and many other advantages that currently are hard to foreseen. Nonetheless, we will coexist with a large number of devices collecting information about activities, habits, preferences, etc. This situation could threaten personal privacy. Distrust could be a barrier to the full development of these new products and services.

Internet of Things reaches its most representative meaning by the Smart Cities providing the necessary solutions to improve the management of modern cities by means of more efficient tools. These tools require gathering citizens’ information about their activity, preferences, habits, etc. opening up the possibility of tracking them. Thus, privacy and security policies must be developed in order to satisfy and manage the legislative heterogeneity surrounding the services provided and comply with the laws of the country where they are provided.

The objective of this thesis is to provide a feasible solution to ensure the security and privacy of personal data on the Internet of Things through resulting techniques from the collaboration between business, legislative and technological areas so as to give confidence to all stakeholders and resolve the possible conflict of interest between them, as well as to manage the legislative heterogeneity.

Whereas most of these services are based on wireless sensor networks, and these networks have significant resource constraints, the proposed management system is also able to cover the security and privacy requirements considering those constrains.

1 Introducción

1.1. Motivación.

La evolución de Internet hacia un intercambio inteligente de información entre objetos [1] posibilita la creación una nueva gama de productos y servicios. Por ello se espera un gran aumento de la cantidad de interconexiones entre dispositivos, en su mayoría inalámbricos, esperándose que se genere una gran cantidad de información. Serán necesarias nuevas arquitecturas de red con suficiente capacidad e inmunidad a la ruptura de la seguridad y a la invasión de la privacidad de las personas. Por lo tanto será necesario elaborar mecanismos que proporcionen entornos seguros y fiables, que eviten que los usuarios perciban, que la utilización estos servicios les hacen vulnerables ante personas u organizaciones oportunistas que puedan obtener beneficio vulnerando su privacidad.

En la investigación realizada sobre la seguridad y privacidad en el campo de "**Internet de las Cosas", o *Internet of Things (IoT)***" en inglés (abreviatura que se utilizará a lo largo de la tesis), se ha podido comprobar la enorme interdependencia entre la selección de los mecanismos y contramedidas de seguridad y privacidad, la legislación que se debe aplicar a un determinado servicio final en IoT, y las necesidades comerciales entre las que se encuentra que los costes deben ser tan bajos como sea razonablemente posible.

El estudio se inició efectuando un análisis del proceso de selección de los mecanismos de seguridad y privacidad que se realizaron durante la especificación y diseño de varios productos y servicios por dos grandes empresas[1] multinacionales del sector. La selección de los mecanismos y contramedidas se realizaban en base a las soluciones tecnológicas aportadas por los expertos en seguridad, que se adecuaban a los requisitos legales obtenidos mediante la contratación de los servicios de asesoría jurídica de empresas consultoras líderes en el campo de la legislación en Internet. Del estudio realizado del proceso de desarrollo de servicios se descubrieron un conjunto de oportunidades de mejora de gran impacto, a continuación se enumeran las más significativas:

1) El alto coste de dichas consultorías tanto en términos económicos, como en "*time-to-market*". Algunos de estos factores pueden terminar siendo limitantes.

[1] Estas empresas, aunque no quieren ser mencionadas, nos prestaron su apoyo.

2) A veces los costes asociados a la seguridad hacen inviable la implantación del producto o el servicio, provocando la cancelación del desarrollo del mismo tras unos gastos significativos de recursos, aún en el caso de rediseñarlo, se acarrean unos costes asociados importantes.

3) Una de las preocupaciones que manifestaron las empresas se centraba en lo relativo a los costes asociados a las reclamaciones, quejas, sanciones y deterioro de la imagen de marca que supone el impacto provocado por los fallos en la seguridad y privacidad.

4) Apuntaron la conveniencia de disponer de un simulador con el que poder ensayar nuevas ideas de productos y servicios, que les pueda dar una visión de los requisitos de seguridad y protección de datos, para realizar una evaluación de los costes y viabilidad previa al inicio de la fase de desarrollo.

5) La heterogeneidad de los marcos legislativos en los diferentes países en que estas empresas operan, representa un importante problema para ellos. Esta heterogeneidad legislativa afecta incluso a un mismo servicio, dependiendo de la utilización que se realice del mismo [2,3]. Esto también sucede cuando un servicio se diseña como una combinación de otros existentes.

6) La actualización ante cambios legislativos que afectan a servicios ya implantados, o ante un posible cambio en el nivel de alarma o alerta en la ciudad, que pueda implicar cambios en los niveles de seguridad y la privacidad en los servicios, genera unas actuaciones que actualmente no son sencillas.

7) Desde el ámbito político se comentó que podría ser muy útil para los agentes implicados en el desarrollo de la legislación, el hecho disponer de una herramienta que permitiera conocer el impacto que puede tener un determinado cambio legislativo (tanto en términos de seguridad y protección de datos, como para evaluar los posibles costes asociados).

8) En el ámbito de las asociaciones de consumidores, se manifestó que el usuario (cada vez es más exigente para dar su confianza), lo que busca es tener garantías de que sus datos, su información, su intimidad, y su seguridad no se vean comprometidas por el hecho de usar o no, esta nueva gama de productos y servicios.

Se pudo apreciar la existencia de una gran actividad investigadora sobre la seguridad y privacidad en IoT, que ha generado una gran cantidad de literatura al

respecto. Hay un gran número de trabajos que proporcionan mecanismos, contramedidas y soluciones tecnológicas contra las amenazas y los ataques a la seguridad y la privacidad. Toda esta literatura se puede dividir en tres grandes áreas de conocimiento (negocio, jurídica y tecnológica). El área de negocio intenta desarrollar sus ideas aumentando así su catálogo de servicios, mientras el área tecnológica desarrolla soluciones técnicas para hacer realidad estos servicios, por otra parte el área jurídica resuelve los conflictos una vez que se han producido problemas de seguridad y privacidad para los usuarios. Realmente la secuencia lógica para evitar incidencias, sería que a partir del conocimiento de los detalles del servicio de IoT que se quiere desarrollar, y del conociendo de los imperativos legales concretos que deban aplicarse (obtenidos y validados de forma oficial), éstos se apliquen mediante las soluciones tecnológicas adecuadas.

Tras consultar la literatura relevante sobre este tema y realizadas consultas a miembros relacionados con el área de conocimientos jurídicos de la "Internet Society", a partidos políticos, a sindicatos, etc., la idea de la cooperación entre las tres áreas de conocimiento (negocio, jurídica y tecnológica) se vio que podría dar unos resultados espectaculares y comenzó a tomar forma. Este concepto de canalizar los requisitos de seguridad y privacidad a través de un sistema colaborativo es una contribución original de esta tesis. La colaboración entre áreas se materializa en la aportación del conocimiento útil empresarial, legislativo y tecnológico para que pueda ser utilizado por un sistema experto para dar una respuesta colegiada a los servicios finales.

No se pudo encontrar ningún sistema ni paquete integrado que se adaptara a la automatización que se buscaba. Lo más parecido eran los "Sistemas Expertos Legales", aunque éstos se centran en la resolución de conflictos y en el análisis legislativo. El sistema experto que se propone se inspira básicamente en el libro de Cuadrado Gamarra sobre sistemas expertos en el ámbito jurídico [4], y los artículos de Charles Stevens [5] y Venkateswarlu [6], así como en sus referencias relacionadas sobre "Sistemas Expertos Legales". En esta tesis no se trata de resolver los conflictos legislativos como es el caso de las obras antes mencionadas [4-6], lo que se busca, es obtener el conocimiento legislativo clave necesario sobre seguridad y privacidad, para poder conocer los imperativos legales necesarios, para aplicarlos a un servicio de IoT concreto.

1.2. Objetivos

El objetivo general de esta tesis es proponer un sistema experto que genere las políticas de seguridad y privacidad necesarias y suficientes para cumplir los requisitos legales de privacidad en los servicios de IoT.

Se centrará en dar soluciones a las vulnerabilidades técnicas propias de las **"**Redes Inalámbricas de Sensores" (*Wireless Sensor Network WSN)* en inglés, abreviatura que se utilizará a lo largo de la tesis. No es objetivo de esta tesis tratar aspectos (que aunque son muy importantes, ya están suficientemente tratados), como son la seguridad de los servidores, antivirus, copias de seguridad, y otros.

Los objetivos específicos de la tesis se distribuyen en cada uno de los tres ámbitos, el de negocio, el jurídico y el tecnológico.

Objetivos específicos en el ámbito de negocio:

Analizar el entorno de negocio para determinar las entradas del sistema experto.

- Determinar las entradas al sistema experto.
- Analizar la realimentación que el sistema experto debe ofrecer al ámbito de negocio, para determinar el rendimiento del sistema en cuanto a seguridad y privacidad desde el punto de vista de negocio.

Objetivos específicos en el ámbito del cumplimiento de la legislación:

- Determinar los imperativos legales de privacidad que se deben aplicar a la información que necesita ser protegida, bien por ser considerarla "sensible", o bien porque en combinación con otra información se convierte en "sensible".
- Analizar la realimentación que el sistema experto debe ofrecer al ámbito jurídico, para determinar el rendimiento del sistema en materia de seguridad y privacidad (Determinar en qué grado se cumple o incumple la legislación sobre protección de datos personales).

Los objetivos específicos tecnológicos se centran en:

- Seleccionar los mecanismos de seguridad y privacidad más adecuados, con los criterios de máxima economía de recursos, mayor adaptación y efectividad para el caso de uso.

- Analizar la realimentación que el sistema experto debe ofrecer al ámbito tecnológico, para determinar el rendimiento del sistema en cuanto a seguridad y privacidad desde el punto de vista técnico.

1.3. Estructura del documento

El capítulo primero de este documento muestra una introducción que incluye la motivación y los objetivos de la tesis.

En el segundo capítulo se realiza un estudio del estado del arte sobre la seguridad y privacidad en los productos y servicios en Internet de las Cosas, así como las conclusiones más relevantes.

En el capítulo tercero se describe el sistema de protección de datos personales para Internet de las Cosas.

En el cuarto capítulo se realiza la validación del sistema, analizando los resultados en diferentes escenarios.

En el capítulo quinto se describen las mejoras obtenidas respecto al estado del arte inicial, las conclusiones y los trabajos futuros,

Finalmente se incluye la bibliografía utilizada, una tabla de acceso rápido a los documentos utilizados en esta tesis, y una lista de acrónimos.

2 Estado del arte

2.1. Estado del arte de la privacidad en IoT

Como se mencionó en el capítulo anterior al definir los objetivos, este estudio se centrará en los servicios de IoT que utilizan las redes WSN. En las WSN, los nodos se pueden equipar con uno o varios sensores, y actuadores para realizar actuaciones ante ciertos estímulos, o bien para disparar alarmas. La parte sensorial de los nodos se encarga de capturar medidas físicas del entorno que transforman en datos y envían a los nodos sumideros (sink). Estos datos se transforman en información y en conocimiento en la estación base (EB). A partir de este conocimiento se pueden gestionar las actuaciones para responder adecuadamente a ciertos estímulos, o informar de la situación del entorno creando eventos de mayor nivel para dar una visión aumentada de dicho entorno. Es posible estimular actuaciones automáticas, semiautomáticas o manuales para reaccionar a las anomalías que se detectan en el entorno sometido a monitorización. Los servicios de IoT ofrecen la capacidad de observar, gestionar y actuar sobre el mundo real a través del mundo virtual. Para ello se necesita obtener información útil del mundo real a través del conocimiento adquirido de los datos brutos recopilados y posteriormente enriquecidos con información adicional de contexto. Este enriquecimiento suele hacer uso de metadatos, de forma que estos datos y sus metadatos asociados son almacenados para su tratamiento y posterior análisis. Cuanta más información de contexto se tenga, mejor interpretación se puede hacer de la realidad, permitiendo gestionar el mundo real a través del mundo virtual con una percepción aumentada.

Hay servicios de IoT que gestionan infraestructuras críticas, otros son críticos para algún ámbito de la sociedad, otros son útiles para apoyar la actividad humana, etc. En cualquier caso las actuaciones que se llevan a cabo sobre la realidad, se basan en la información obtenida y procesada. En el caso de producirse ataques a la información recopilada o procesada, puede tener como consecuencia la realización de actuaciones sobre una realidad falseada (centrales nucleares, embalses de agua), pudiendo provocar resultados catastróficos.

Otra gama de servicios sensibles a los ataques son los que recopilan información sobre las personas y su entorno. Estos ataques pueden provocar grandes perjuicios a las personas y crear anomalías en el servicio que utiliza el usuario falseando la información o denegando el servicio, esto puede suponer desde un fraude, hasta provocar un riesgo real para la vida del usuario. Por otra parte el espionaje o robo de información personal de los usuarios, podría dar lugar a que esta

información sea tratada y utilizada por terceros para obtener beneficio a costa de los derechos de los usuarios. Esta información sensible está regulada por la legislación vigente.

La pérdida de la confianza y la sensación de invasión de la intimidad de los usuarios podría ser un obstáculo para el pleno desarrollo de esta gama de productos y servicios. Una de las mayores preocupaciones es que el propio usuario pueda actuar como “sensor” proporcionando información sobre sí mismo, sus movimientos, hábitos, preferencias, actividades, etc. con su smartphone y demás dispositivos inteligentes (como los dispositivos embebidos en la vestimenta). El temor consiste en ser analizados e incluidos en listas de perfiles que podrían ser utilizados en muchas áreas, principalmente en estudios y actuaciones de marketing, segmentando a las personas directa o indirectamente, o bien ser utilizados con fines delictivos. En cualquier caso el usuario desconoce la utilización que se hace con su información personal.

Del estudio de los actores mencionados en la IoT, se ha podido comprobar que el área de negocio normalmente son los promotores de los servicios (con la finalidad de obtener un beneficio económico o social), mientras que el área jurídica es el garante de los derechos de las personas. Finalmente el área tecnológica que es quien implementa técnicamente el servicio. Se ha podido apreciar la coexistencia de tres estados del arte, uno para cada una de las áreas.

Tal como se comenta en los artículos [2,3] generados a partir de esta tesis, se pudo comprobar que el estado del arte incluía tres perspectivas: 1) La perspectiva comercial relacionada con los productos y servicios, las empresas se centran en crear nuevas ideas y servicios para comercializarlos. 2) La perspectiva tecnológica, que se centra en proporcionar las mejores y las más eficientes soluciones. 3) La perspectiva legislativa, que no siempre es homogénea para los diferentes mercados, lo que provoca un impacto muy significativo para las empresas relacionadas con los sectores que realizan estas actividades.

Por otra parte la velocidad de cambio con la que cada una de estas áreas avanza es muy diferente, la percepción general es que la regulación va por detrás de los avances tecnológicos provocando riesgos potenciales para las personas e infraestructuras críticas. A continuación se estudia cada uno de estos tres estados del arte.

2.2. Estado del arte en el ámbito de negocio o promotor

Se comenzará enumerando los tipos de servicios de IoT que se suelen comercializar y promocionar en la actualidad, en ellos se centra el interés actual del mercado:

- *Fábrica Inteligente*: Brinda a las empresas la capacidad de realizar un seguimiento de todos sus productos, reduciendo así sus gastos operativos y mejorando su productividad mediante la optimización de sus recursos empresariales, y facilitando el mantenimiento de la maquinaria mediante la monitorización en tiempo real de su estado y rendimiento.

- *Transporte/Logística*: Cuyo objetivo es mejorar la cadena de suministro, el posicionamiento global y la identificación automática de las mercancías.

- *Minoristas (Retail)*: Dirigido a clientes, tiendas y empresas, las aplicaciones de IoT permiten comparar precios de productos, buscar otros productos de la misma calidad a precios más bajos, así como promociones.

- *Hogar Inteligente*: Aumenta los niveles de confort disminuyendo a la vez el gasto total, con la lectura remota de contadores (gas, agua y electricidad) se puede controlar la demanda y ofrecer servicios adicionales, con la detección de incendio o la entrada no autorizada se pueden dar servicios de seguridad, entre otros.

- *Automatización de edificios*: Mediante el control centralizado de la climatización, del nivel lumínico, de la seguridad, etc. se puede optimizar tanto el funcionamiento individual como conjunto así como los costes.

- *Ciudades Inteligentes*: Para optimizar la gestión de una ciudad mediante monitorización y automatismos inteligentes con la finalidad de reducir costes, mejorando la información y la atención al ciudadano (aparcamientos inteligentes, control de tráfico, alumbrado inteligente, servicios combinados como la gestión de emergencias, etc.) y haciendo sostenible el desarrollo y la calidad de vida.

- *Smart Energy/Smart Grid*: Apoya al hogar inteligente y a la ciudad inteligente. El objetivo es ahorrar energía. En base a la medición inteligente se proporcionan servicios como la rápida detección de interrupciones y la restauración automática

del servicio, un mayor control del consumo por parte de los clientes y facilidades para la gestión de sus facturas.

- *E-Salud*: Con el objetivo del control y la prevención. Se efectúa un seguimiento y control por los especialistas de forma remota, favoreciendo la comunicación médico-paciente, mejorando la atención y la satisfacción del paciente.

- *Teleasistencia médica*: Dirigido a ancianos, a personas con alguna discapacidad, etc. a partir de los parámetros biométricos medidos por sensores permiten la monitorización remota y permanente, pudiendo realizar diagnósticos y disparando alarmas o alertas si se detectan situaciones de emergencia.

- *Monitorización medioambiental*: Con el fin de supervisar el entorno o bien colocados en los seres vivos. Se trata de realizar un control sobre el estado del medioambiente.

- *Monitorización preventiva*: Para realizar una supervisión continua de los parámetros que puedan permitir realizar una predicción (mediante software capaz de extrapolar la evolución de los parámetros medidos) de problemas potenciales en el mundo real y ofreciendo la capacidad de realizar las actuaciones necesarias que eviten que se produzcan.

- *Agricultura*: Su finalidad consiste en mejorar la productividad de las cosechas, midiendo parámetros como el grado de humedad del suelo para optimizar el riego, la humedad de las hojas para predecir hongos, o bien midiendo la radiación solar para determinar el mejor momento para las cosechas.

- *Generación de nuevos servicios*: Control, descripción, virtualización …

Desde el punto de vista empresarial, el ecosistema actual de IoT está tan fragmentado y es tan complejo que está retrasando la decisión de las empresas y consumidores, porque la toma de decisiones en estas condiciones se considera que implica un alto riesgo. Las grandes empresas del sector se están aliando, como AT&T, Cisco, GE, IBM e Intel formando el "*Industrial Internet Consortium for IoT standards*", cuya finalidad es minimizar los riesgos de integración en las aplicaciones de IoT y avanzar en la definición de estándares. En la situación actual para las empresas el mercado de servicios de IoT, ni es el único ni el más importante, porque los ingresos todavía son pequeños comparados con las expectativas.

En la conferencia TedxSF de San Francisco (US) en 2014, Rachel Kalmar enumeró los principales desafíos en IoT que a continuación se relacionan:

- Falta de una infraestructura compartida; existen pocas plataformas de código abierto para IoT, cada dispositivo depende de su propia plataforma y ecosistema.
- Falta de Estándares; aunque hay iniciativas al respecto en la UIT. Por su parte el Comité Técnico de M2M de la ETSI, está tratando de agrupar las múltiples tecnologías y estándares existentes en un escenario muy fragmentado, intentando armonizar y completar los vacíos normativos.
- Duración de la batería; hay una necesidad de aumentar la duración de las baterías a partir de fuentes de energía no convencionales.
- Control de los datos; respecto a controlar y decidir quién tiene acceso a los datos y qué se hace con ellos.
- Intercambio de información; el mercado de los datos supone una amenaza creciente para los usuarios.

En España ocurre algo similar al resto del mundo, siendo válido lo anteriormente expuesto. Durante estos años los Operadores de Telecomunicación han implantado soluciones M2M en sectores tales como Gestión de flotas, máquinas de vending, ascensores, agricultura de precisión y en el sector de la seguridad. El objetivo ha sido la búsqueda de nuevos ingresos mediante las nuevas altas de líneas “M2M” con SIM de datos, para afrontar la continua reducción de ingresos en los servicios de voz y datos SMS.

Debido a las predicciones optimistas de crecimiento de M2M, las Telcos están ampliando su oferta y ofreciendo además de conectividad, soluciones empaquetadas de servicios para los clientes, buscando oportunidades en diversos sectores como el de la energía con los Contadores Inteligentes, la automoción con el coche conectado, la salud o las ciudades inteligentes. Los Operadores de Telecomunicaciones en España también han efectuado alianzas con los otros agentes (fabricantes de los módulos que albergan las SIM, de redes inalámbricas de sensores, de plataformas de datos, fabricantes de aparatos o distribuidores). Las WSN están potenciando esta industria, gracias al desarrollo de las ciudades inteligentes con compañías como Libelium, Sayme o TST y empresas españolas como Indra, Zemsania, Carriots, Telefónica dedicadas a las plataformas y a construir aplicaciones y servicios de IoT.

Por otra parte los Integradores de Sistemas están interesados en la visión conjunta de IoT junto con servicios tanto en Cloud como Big Data.

La visión y las previsiones de las empresas respecto al futuro de IoT se basa en explotar la conexión a diferentes fuentes y recursos de información de una manera mucho más estrecha. Se espera que el número de dispositivos conectados crezca exponencialmente durante los próximos años integrándose en la vida cotidiana de las personas e impulsando la demanda de nuevas soluciones que den lugar a nuevos modelos de negocio.

La visión de *Cisco Internet Business Systems Group* en su hoja técnica [7] de abril de 2011, es que IoT representa la próxima evolución de Internet y cuenta con el potencial de transformar nuestro mundo. Dos años más tarde, Cisco lanza otro documento [8], hablando del gran impacto potencial a largo plazo de IoT en términos de valor económico y en la transformación de la manera de vivir y de trabajar. Sus ejecutivos creen que impulsará el crecimiento del empleo y el aumento de salarios, a la vez que catalizará mejoras en seguridad de la información. Recalcan la idea de que las organizaciones aplicarán esta tecnología en sus estrategias para mejorar sus recursos humanos y sus procesos de negocio.

Por otra parte *McKinsey Global Institute*, en su informe [9] comenta que las aplicaciones de IoT pueden tener un impacto económico directo entre 2.7 billones y 6.2 billones de dólares al año en 2025, y prevén que entre el 80% y el 100% de los fabricantes utilizarán aplicaciones de IoT con un impacto económico potencial de 2.3 billones de dólares para el sector de fabricación. Consideran la IoT como una de las tecnologías que alteran los modelos actuales de negocio.

También se refiere *McKinsey* a que la posibilidad de recopilar datos de una ingente variedad de sensores y casos de uso, requerirá una infraestructura de comunicaciones eficaz para transmitir información e instrucciones de control, con potentes prestaciones de análisis de datos para conseguir perspectivas significativas. Se plantea que para capturar esta oportunidad de crear valor, los fabricantes necesitan un replanteamiento general, desde cómo se crean los productos y servicios hasta cómo funcionan y se reparan. Las nuevas capacidades de los productos inteligentes conectados abren la puerta a una nueva forma de competir.

En el congreso "*Global Conference on CyberSpace*" de abril de 2015 en "*The Hague, Holanda*", se trató sobre las extraordinarias oportunidades para el crecimiento económico y el desarrollo social, y que se ha convertido en una parte vital de las

sociedades de todo el mundo, lo que impulsa la aparición de nuevos retos. En este congreso se definieron los retos y oportunidades existentes, abordándolos desde la perspectiva de la seguridad, de la libertad, y de los beneficios sociales y económicos. También se analizaron los nuevos grupos de interés y los tradicionales, dando como resultado la publicación de "la declaración de la presidencia" [10]. En su punto cuarto expresa la necesidad de asegurar que los derechos humanos, junto con la libertad de expresión y el derecho a la privacidad, se deben proteger de forma equivalente tanto en línea como fuera de línea con un compromiso inequívoco. En su punto trece, se apoya de forma explícita al Foro de Gobernanza de la Internet. En su punto treinta y uno se reafirma el importante rol de la ONU en el mantenimiento de la paz internacional y de la seguridad en el ciberespacio. Finalmente en el punto cuarenta y dos, se afirma que el derecho a la privacidad debe ser respetado de forma equivalente tanto fuera de línea, como en línea y reconoce que el derecho del individuo a la privacidad es importante para salvaguardar otros derechos humanos, incluyendo la libertad de expresión, de reunión y asociación.

También se publicó una declaración conjunta[2] de los miembros de la Comunidad técnica de la Internet e Internet Society, matizando que la protección de los derechos humanos así como la seguridad en línea son conceptos complementarios, y se lanza el sitio *Internet.nl* dedicado a comprobar la calidad y fiabilidad de la conexión a la red.

En la Conferencia del XXI encuentro de ICT y Digital Media en Barcelona de junio de 2015, el presidente y consejero delegado de Investigación y Desarrollo de Telefónica augura que IoT generará nuevos modelos de negocio y formas de consumo, asegurando que la conectividad de los objetos permitirá diluir las fronteras entre el mundo físico y el digital, creando nuevas maneras de adquirir productos y apareciendo nuevos tipos de modelos de negocio, como Bcommerce (Botton Commerce) y Bservices, el Bsupport (pulsa y voy). Comenta también que estos nuevos negocios abren la puerta a nuevos servicios en los que el distribuidor perderá protagonismo. Señaló que para posibilitar la conexión de tal cantidad de objetos a nivel mundial, sería necesario reducir los costes de las tecnologías y estandarizar un sistema de aplicación global, y recuerda que Europa ha adoptado la plataforma Fiware[3] para implantar la conectividad de los objetos.

[2] http://www.internetsociety.org/news/statement-members-internet-technical-community-after-global-conference-cyberspace-2015-gccs2015
[3] https://www.fiware.org/

2.3. El estado del arte en el ámbito legal

Los productos y servicios de IoT se basan en la información recopilada y procesada procedente de una o varias fuentes. Esta información puede referirse al medioambiente, a personas, a servicios e infraestructuras críticas, pudiendo incluir elementos de información sensibles por motivos de seguridad y privacidad. Estos elementos de información sensibles se consideran “activos” sometidos a marcos legislativos que los protegen mediante la asignación de unos determinados niveles de seguridad y privacidad. Esta protección da lugar a unos imperativos impuestos por el marco legal, al que se encuentra sometido el servicio final.

En el ámbito europeo el Convenio del Consejo de la Unión Europea n. 108, Estrasburgo 28/1/1981 [11], estableció unos criterios comunes de protección de datos para todos los miembros de la CE, coordinado por la Directiva 95/46/CE del Parlamento Europeo de 24/10/1995 [12].

En su informe sobre la Directiva de protección de datos de 24/02/2004 [13], la UE reconoce la heterogeneidad legislativa existente en sus países miembros y enfatiza la necesidad de que los estados e instituciones europeas adopten un nivel equivalente de protección de los derechos de las personas. Resalta que esta heterogeneidad de las legislaciones nacionales en materia de protección de datos, dificulta el desarrollo del mercado interior europeo.

Como resultado de las líneas de actuación establecidas por el Parlamento Europeo en la Comunicación del Comité Económico y Social Europeo (2009) [14], Europa camina hacia un marco normativo común con la Propuesta de reglamento general de protección de datos [15]. Una vez aprobada será de aplicación directa en dos años para toda la Unión Europea. Este Reglamento afectará a quienes hagan tratamiento de los datos de carácter personal y tengan establecimiento en algún estado miembro, aun si el tratamiento de la información se realiza fuera de la Unión Europea. Respecto a las empresas no establecidas en Europa les afectará, en caso de que traten datos personales para prestar bienes y servicios a residentes en la UE.

El Reglamento incluye los conceptos de responsabilidad, privacidad por diseño (o desde el diseño), privacidad por omisión, evaluación del impacto sobre privacidad, y la necesidad de implantar unos criterios de gobierno interno y operativos enfocados a la gestión de riesgos, así como el derecho al olvido.

El grupo de trabajo *Working Party 29 (WP29)* ha aprobado el primer Dictamen 8/2014 de 16/09/2014 [16], sobre los *"nuevos desarrollos en la Internet de las Cosas"*, cuya elaboración ha sido liderada por la Agencia Española de Protección de Datos (AEPD) junto con la autoridad francesa *Commission Nationale de l'informatique et des libertés (CNIL)*. WP29 analiza tres escenarios:

- "tecnología para llevar puesta" o "informática en la vestimenta" (*wearable computing*);
- dispositivos que registran información sobre la actividad de las personas;
- domótica.

Se identifica y se alerta de los riesgos que estos productos y servicios pueden plantear para la privacidad de las personas, definiendo responsabilidades y ofreciendo recomendaciones. El documento destaca que aunque los objetos recopilen piezas aisladas de información de diferentes fuentes, su análisis conjunto puede revelar patrones de la vida de las personas. El 10 de octubre de 2014 se editó la Recomendación [17], relativa al *"Modelo de evaluación del impacto sobre protección de datos para redes inteligentes y sistemas de contador inteligente"* estableciendo un método para impulsar el entendimiento entre la legislación y la realidad técnica.

El Reglamento general de protección de datos homogenizará la legislación europea en materia de protección de datos personales, aunque en un mercado de cobertura mundial todavía será necesario convivir con la heterogeneidad legislativa.

2.4. Estado del arte en el ámbito tecnológico

En el ámbito de seguridad en las comunicaciones de datos, se utiliza como base la Recomendación X.800 de la ITU sobre "la seguridad en las redes de comunicación de datos" [18]. Según esta recomendación los elementos susceptibles de ser protegidos son las informaciones y los datos sensibles (incluidos los relativos a las medidas de seguridad, como son las contraseñas), los servicios de comunicación, y el procesamiento de datos. A los elementos mencionados se asigna un nivel de seguridad y privacidad acorde con las necesidades del servicio final y de la información involucrada [19]. Esto es válido tanto para los servicios finales prestados por WSN individuales, como para el servicio holístico compuesto por un conjunto coherentemente integrado de servicios relacionados (en una ciudad inteligente, por ejemplo). Este nivel de seguridad se materializa en la implementación de unos

determinados servicios de seguridad que se construyen mediante un conjunto de mecanismos y contramedidas capaces de contrarrestar los ataques o amenazas. La Recomendación X.800 define los siguientes servicios de seguridad:

- autenticación: para identificar la entidad comunicante y la fuente de datos;
- control de acceso: para prevenir el uso no autorizado de los recursos;
- confidencialidad de los datos: para protegerlos contra la revelación no autorizada;
- integridad de los datos: para garantizar que no han sido alterados o destruidos de una manera no autorizada;
- no repudio: para dar prueba del origen de los datos o de entrega de los mismos;
- disponibilidad: para garantizar la continuidad de la accesibilidad y utilización por las entidades autorizadas.

Estos servicios de seguridad se construyen mediante mecanismos de seguridad, bien solos o combinados, como son:

- cifrado;
- firma digital;
- mecanismos para el control del acceso;
- mecanismos de integridad de datos;
- intercambio de autenticación;
- relleno de tráfico;
- control de encaminamiento;
- notarización.

La recomendación X.800 ilustra la relación entre los servicios y los mecanismos de seguridad.

Dado que las WSN son redes de recursos limitados, se utilizan protocolos de bajo consumo y procesamiento ligero, por lo que se opta por realizar un diseño a medida para obtener la cobertura de seguridad y privacidad necesaria, sin perjudicar a la calidad del servicio final que se ofrece.

Los mecanismos más utilizados son la criptografía, los esquemas de autenticación y distribución de claves, los mecanismos de enrutamiento y agregación segura de datos, los mecanismos de localización segura, los sistemas de detección de intrusiones, y los esquemas basados en confianza, entre otros. Estos mecanismos de seguridad consumen recursos en redes donde ya son bastante escasos, en este sentido hay incluso ataques cuyo objetivo principal es sobrecargar los nodos para provocar un consumo extra [20]. La necesidad de desarrollar mecanismos ligeros y eficientes ha estimulado la existencia de una gran actividad investigadora que ha dado como resultado multitud de soluciones que se pueden aplicar a casos concretos. En base a los mecanismos de seguridad y privacidad disponibles en los estándares, se desarrollan otros más complejos y adaptados a las necesidades concretas.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) [21] creó el grupo de trabajo *Task Group 4* para el ámbito de las redes de área personal de baja velocidad, con la finalidad de definir una interfaz radio de bajas prestaciones que se pudiese compartir. Este grupo desarrolló la familia de especificaciones IEEE 802.15.4 para los protocolos de capa física y de control de acceso al medio de la interfaz radio [22]. Por otra parte los fabricantes crearon el foro de estandarización ZigBee Alliance [23] que especificó una pila completa de protocolos utilizando para las capas física y MAC las especificaciones IEEE 802.15.4. En el entorno de Internet, IETF [24] ofreció una capa de adaptación que permitía el transporte de IP (versión 6) sobre interfaces radio IEEE 802.15.4 (6LoWPAN WG) [25]. Esta actividad continuó con la definición de soluciones de encaminamiento (ROLL WG) [26] así como funcionalidades y aplicaciones de nivel superior *(CoRE WG*). Otros fabricantes y desarrolladores se enfocaron hacia Bluetooth (Bluetooth SIG) [27] con la modificación del estándar (Bluetooth Low Energy). Por su parte los fabricantes siguen aportando soluciones propietarias y creando foros para promocionar sus soluciones (Z-Wave Alliance [28], Wavenis Open Standard Alliance [29], etc.).

ZigBee define una arquitectura de seguridad completa que se añade a las funcionalidades del estándar IEEE 802.15.4 [30]; lo mismo pasa en el caso de 6LoWPAN [31]. Con respecto a BT-LE [32], la capa de enlace proporciona el cifrado y

la autenticación mediante el uso de AES-128 y CCM. La visión de la situación se resume en la tabla 1.

Servicios De seguridad	**ZigBee**	**6LoWPAN**	**BT-LE**
	Totalmente especificado (incluyendo la gestión de claves, IEEE 802.15.4)	Análisis de seguridad actualmente en desarrollo. Hasta el momento, 6LoWPAN se basa en la seguridad IEEE 802.15.4	Cifrado y autenticación.

Tabla. 1. Servicios de seguridad (ZigBee, 6LoWPAN and BT-LE).

Otro estándar muy utilizado es IEEE 802.11 (Wi-Fi), que define métodos para lograr la configuración segura de una red inalámbrica, así como los niveles de seguridad. Entre los protocolos disponibles están WEP, WPA, WPA2 y entre los mecanismos disponibles se encuentran los ACL, Cortafuegos (Firewall) etc. Como solamente cubren parte de los aspectos que habitualmente se necesitan, surgen soluciones más específicas como son los sistemas de detección de intrusiones.

El estándar más empleado es la pila de protocolo IEEE 802.15.4/ZigBee, que cuenta con 8 suites de seguridad disponibles [33] agrupadas en 4 grupos, que se utilizan como base para las operaciones criptográficas [34]. Estos grupos son: 1.- “Sin seguridad”; 2.- “Sólo cifrado” AES-CTR [34] proporcionando *confidencialidad*; 3.- “Sólo autenticación/integridad” “AES-CBC-MAC” [35] ofreciendo *autenticación e integridad*. 4.- “Cifrado + autenticación/integridad” “CBC-MAC-CCM” [36] que ofrece *confidencialidad, autenticación e integridad*. Por otra parte IEEE 802.15.4 también define dos mecanismos para mejorar el soporte a la autenticación y a la integridad de las comunicaciones. El *Control de acceso,* para lo que cada dispositivo mantiene una Lista de Control de Acceso (ACL) con los dispositivos autorizados, y la p*rotección contra repetición/reproducción*, pero no especifica los mecanismos de gestión de claves, por tanto deben de realizarse en las capas superiores.

ZigBee define el *establecimiento de claves, el transporte de claves, la protección de tramas* y la *gestión de dispositivos,* para una red IEEE 802.15.4. [37]. Así, se define una arquitectura de seguridad que se añade a las funcionalidades de IEEE 802.15.4 [30].

La defensa estándar contra los ataques de escuchas, inyección y modificación de los paquetes, es la criptografía. La utilización de las técnicas de algoritmos de clave pública, Diffie-Hellman [38] o las firmas RSA [39] tienen un gran consumo de recursos debido a la alta carga computacional. Sin embargo los algoritmos criptográficos de

clave simétrica y las funciones de hash suelen tener menor consumo [40]. Algunos estudios han demostrado que ya es posible aplicar la criptografía de clave pública para ciertas WSN, mediante una buena selección de algoritmos, parámetros asociados, optimización, y técnicas de baja potencia [41-43]. La Criptografía de curva elíptica (ECC) ofrece una seguridad equivalente con un tamaño de clave mucho menor, reduciendo el procesamiento y la comunicación (RSA con claves de 1024 bits es equivalente a ECC con claves de 160 bits, y RSA-2048 es equivalente a ECC-224) [44]. Así, la aplicación de la criptografía RSA y ECC [45] se demostró viable para protocolos basados en clave pública en algunos casos.

Un importante reto consiste en la distribución segura de la clave compartida entre las partes comunicantes en los mecanismos criptográficos de clave simétrica. Algunos esquemas de cifrado, como RC4 [46], RC5 [47], IDEA [46], SHA-1 [48], y MD5 [46, 49], fueron evaluados sobre diferentes microprocesadores [50], concluyendo que los algoritmos hash (MD5, SHA-1) tienen una mayor sobrecarga que los algoritmos de cifrado (RC4, RC5 e IDEA). La criptografía de clave simétrica ha resultado ser mejor que la criptografía de clave pública en términos de velocidad y bajo consumo de energía. Se comprobó que Las primitivas que mejor se adaptan a la criptografía de clave simétrica para las WSN de bajos recursos es RC4, por su tamaño de bloque y sencillez de sus operaciones. En caso de disponer de WSN con mayores recursos, se podría utilizar RC5 y RC6 [51].

Respecto a las primitivas de hash, algoritmos tales como SHA-1 [52], SHA-256, RIPEMD-160 [53], y otras primitivas criptográficas tales como los Códigos de Autenticación de Mensajes (MAC) suelen utilizarse para lograr *integridad* y *autenticidad*; pueden conseguirse con el modo CBC-MAC de SKC.

2.4.1. Esquemas de autenticación y de distribución de claves

Tras la realización del despliegue inicial y el descubrimiento de vecinos directos, los nodos WSN necesitan disponer de un *esquema de autenticación* que proporcione autenticidad, por tanto los nodos deben disponer de la información criptográfica necesaria obtenida mediante una distribución segura. Los esquemas de autenticación y de distribución de claves se deben de adaptar a cada tipo de WSN, sus limitaciones hacen ineficiente el establecimiento de claves únicas con todos los nodos [54] y la mayoría de los sistemas criptográficos de clave pública son poco prácticos Diffie-Hellman key agreement [55], firmas RSA [56]. Según R. Rivest [57] los métodos

criptográficos tienen el problema de que el uso de claves largas y fuertes, aumenta el retardo de procesamiento de la autenticación de clave pública, brindando así la oportunidad a un adversario, de realizar ataques de *DoS* [58] contra la autenticación del nodo, enviando solicitudes de autenticación arbitrarias y obligando al nodo receptor a descifrar y cifrar continuamente, provocando el agotamiento de la batería.

Para realizar un diseño de soluciones robustas de autenticación, se debe considerar la posibilidad de que un nodo pueda ser capturando físicamente y se obtenga acceso a todas las claves almacenadas en su memoria [59], exponiendo a la red a sufrir ataques *Sybil* [52]. Frente a este tipo de ataques se puede usar la "Prueba de recursos" bien como parte del procedimiento de autenticación, o bien como una medida periódica de seguridad para mantener la autenticidad. También debe considerarse que debido a la pérdida natural de nodos durante la vida útil de una WSN, debe de contemplarse la reposición de dichos nodos. Esto obliga a que el esquema de autenticación deba de estar preparado para aceptar la autenticación de nuevos nodos que se puedan agregar a la red, lo que implica que la información de *bootstrapping* no se deba borrar tras el despliegue, añadiendo así un riesgo adicional en caso de captura [59]. Otra consideración que debe realizarse es prever la posibilidad de que entre los nodos que se despliegan, no todos sean legítimos y algunos puedan ser maliciosos [60]. Una consideración añadida es que la EB por ser considerada como fuente de confianza, pueda ser objetivo de ataques por lo que el esquema de autenticación debe minimizar su comunicación con ella [54].

2.4.2. Esquemas de distribución de claves en base a la estructura de red

Entre los esquemas de distribución de claves basados en la estructura de red se encuentran el "esquema centralizado de claves", donde una única entidad controla la generación, la regeneración y la distribución de claves (*Key Distribution Center, KDC*) como el esquema LKHW [61]. La EB tiene la función de KDC y todas las claves se distribuyen a partir de ella. La escalabilidad del esquema es escasa, y no proporciona autenticación de datos. Otro esquema es el "esquema distribuido de claves" que utiliza diferentes entidades para gestionar las actividades relacionadas con las claves, tiene la ventaja de no concentrar el riesgo ante fallos. Este esquema permite una mejor escalabilidad.

2.4.3. Esquemas deterministas de distribución de claves

Entre estos esquemas se encuentra el protocolo LEAP (*Localized Encryption and Authentication Protocol*) propuesto por Zhu et al [62] basado en algoritmos de clave simétrica, donde se establecen cuatro tipos de claves para cada nodo (una clave individual compartida con la estación base; un grupo de claves compartidas por todos los nodos de la red; un par de claves compartidas con los nodos vecinos inmediatos, una clave de clúster compartida con múltiples nodos vecinos). Lee y Stinson [63] proponen dos esquemas, IOS (*ID-based one-way function scheme*) y DMBS (*deterministic multiple space Bloms' scheme*), y mostraron el uso de conjuntos de sistemas combinatorios en los esquemas de pre-distribución de claves deterministas [64]. Chan y Perrig [65] proponen un protocolo para facilitar el establecimiento de claves entre cada par de nodos vecinos. En el mecanismo PIKE (*Peer Intermediaries for Key establishment*), cada nodo comparte una pareja de claves con los otros nodos que comparten coordenadas en el espacio, en caso contrario utiliza otro nodo de intermediario con alguna coordenada común para reenviarles una clave. La sobrecarga de comunicación es alta. Huang et al [66] proponen un esquema de establecimiento de clave híbrido, donde los principales cálculos criptográficos se realizan en la EB mientras que en los sensores se realizan las operaciones ligeras de clave simétrica. La autenticación de los sensores y la EB utiliza criptografía ECC estableciendo la legitimidad de la clave pública en base a certificados basados en un esquema de curva elíptica.

2.4.4. Esquemas probabilísticos de distribución de claves

El esquema básico probabilístico de distribución de claves se puede ver en [67], y en [59,68-72] se proponen varios esquemas que consisten en la pre-distribución al azar de claves basados en el intercambio probabilístico de claves entre los nodos. De Pietro et al [56] mejoraron el sistema de gestión de claves mediante la asociación de los índices clave de un nodo con su identidad. Blundo et al [73] presentaron un protocolo basado en polinomios para la pre-distribución del grupo claves. Du et al. presentaron el esquema de *multiple-space key pre-distribution (MSKP)* [71], que utiliza el método de Blom [74]. Liu y Ning [69] propusieron un esquema *polynomial pool-based key pre-distribution (PPKP)*, el esquema tiene tres fases: setup, establecimiento de la clave directa, y establecimiento de la clave de camino. El esquema es escalable

y flexible y resiliente a la captura de nodo, el mecanismo tiene gran sobrecarga de almacenamiento en memoria de los nodos sensores. Hwang y Kim [75] proponen mejorar el protocolo básico de gestión de claves aleatorias [67] mediante la reducción de la cantidad de información necesaria en cada nodo, garantizando una cierta probabilidad de compartir una clave entre dos nodos. Hwang et al. [72] amplíaron el esquema básico de gestión al azar de claves, proponiendo un esquema de *cluster key*. Du et al. [67] propusieron un esquema de pre-distribución de claves que utilizaba el conocimiento del despliegue de la red y establecía células cuadradas y asignándoles un subconjunto de claves del pool de claves global. Estos subconjuntos de claves, se establecen como *pooles* de claves entre células vecinas que compartirán una porción de las mismas. En cada célula, se aplica el esquema básico de gestión al azar de claves. El conocimiento del despliegue hace que la sobrecarga de almacenamiento se reduzca significativamente.

2.4.5. Mecanismos de enrutamiento y agregación segura de datos

Tras la autenticación inicial y el procedimiento de localización [76, 77] se debe tener en cuenta los mecanismos de enrutamiento y agregación segura de datos. Se pueden clasificar según la topología de la red subyacente [76] como; 1- enrutamiento plano; 2- enrutamiento jerárquico; y 3- enrutamiento basado en la ubicación [78]. Estos enrutamientos son vulnerables a los ataques de reenvío selectivo, sinkhole, como se muestra en [79]. El objetivo de un enrutamiento seguro es garantizar la integridad, la autenticación y la disponibilidad de los mensajes. La mayoría de los algoritmos de enrutamiento seguros existentes se basan en la criptografía de clave simétrica, aunque algunos se basan en la criptografía de clave pública [71].

µTESLA (*Micro version del Timed Efficient Streaming Loss-tolerant Authentication protocol*) [80] y sus extensiones [81, 82] proporcionan autenticación de transmisión, y es un protocolo de autenticación SPINS Perrig et al [83]. Liu y Ning [81,82] han propuesto un esquema de cadena de claves a múltiples niveles para la autenticación de difusión, predeterminando y difundiendo los parámetros iniciales requeridos por µTESLA en lugar de utilizar la transmisión de mensajes *unicast*. Zhu et al [62] han propuesto un esquema de la cadena de claves de un solo sentido para la autenticación de emisión de un solo salto (LEAP). Deng et al [84] propusieron un protocolo de enrutamiento tolerante a la intrusión (INENS). Tanachaiwiwat et al. [85] presentaron un protocolo de enrutamiento seguro y confiable para la ubicación de la

WSN (TRANS), para su uso en redes centradas en datos con el fin de garantizar la confidencialidad del mensaje. Papadimitratos y Hass [74] han propuesto un protocolo de descubrimiento de ruta segura que garantiza la detección de la topología correcta en una red de sensores ad hoc.

Newsome et al [53] han descrito la taxonomía del ataque Sybil en diferentes dimensiones: 1- comunicación directa vs. indirecta. 2- Engaño vs. Robo de identidades 3- la simultaneidad. Algunas técnicas para defenderse contra el ataque Sybil utilizan técnicas de pre-distribución de claves aleatorias [86, 67,59]. Respecto al ataque de replicación de nodo, Parno, Perrig y Gligor [87] han propuesto dos algoritmos que trabajan a través de las acciones colectivas de múltiples nodos: 1- multidifusión aleatoria; 2- multidifusión línea seleccionada (para detectar repeticiones). Para reducir las comunicaciones Parno et al [88] han propuesto un algoritmo alternativo, la multidifusión que se basa en el protocolo de *rumor routing*.

2.4.5.1. Mecanismos contra ataques de análisis de tráfico

Los mecanismos de defensa contra los ataques de análisis de tráfico se han catalogado según dos tipos de ataques: 1- ataque de supervisión; y 2- ataque de correlación. Para prevenirlos hay cuatro técnicas; 1- un esquema de enrutamiento a múltiples padres, para que los patrones de enrutamiento hacia la EB sean menos previsibles. 2- una trayectoria aleatoria controlada multi-salto de un paquete a través de la WSN hacia la EB, lo que distribuye el tráfico haciendo que el ataque de monitorización sea menos eficaz. 3- Introduciendo caminos falsos aleatorios para confundir al adversario a medida que el paquete avanza hacia la EB, mitigando así la eficacia de los ataques de correlación. 4- Creando múltiples áreas al azar para engañar al adversario sobre la verdadera ubicación de la EB, aumentando así la dificultad de los ataques de monitorización.

Estas cuatro estrategias combinadas crean un mecanismo robusto frente a los ataques análisis de tráfico.

2.4.5.2. Mecanismos de agregación segura de datos.

Los mecanismos de agregación segura de datos optimizan el consumo de energía, ya que la comunicación de los datos representa alrededor del 71% del coste de procesamiento y comunicación en los protocolos SNEP [80]. La agregación segura

de los datos requiere *autenticación, confidencialidad, e integridad*, así como la cooperación entre los nodos sensores para identificar los sensores sospechosos de estar comprometidos. En [89], se presentó un algoritmo basado en agrupaciones (*clustering*) que utiliza la técnica de difusión dirigida. En [90] se propone un mecanismo llamado TAG, de agregación de datos con un lenguaje como el SQL, para generar consultas en la WSN. La EB genera la consulta y los nodos sensores envían la respuesta a través de rutas construidas en base a un árbol de enrutamiento, agregando los datos según una función de agregación definida en la consulta inicialmente enviada.

Hu y Evans [91] propusieron un protocolo de agregación segura que utiliza el protocolo µTESLA, resistente tanto a dispositivos intrusos como a dispositivos que tienen la clave comprometida, pero es vulnerable cuando el nodo padre y uno de sus hijos se vea comprometidos. Przydatek et al [80] presentaron un marco de agregación de la información segura (*SIA - secure information aggregation*) que consta de tres categorías de nodos; home server, EB y nodos sensores.

Deng et al [86] propusieron un conjunto de mecanismos SINP (*Securing In-Network Processing*), para afrontar la exigencia de que los nodos sensores autentiquen comandos difundidos desde los agregadores y que estos autentiquen los datos producidos por los sensores antes de que sean agregados.

Cam et al [92-94] propusieron el protocolo ESPDA (*Energy-efficient Secure Pattern-based Data Aggregation*), que se aplica a redes de sensores jerárquicas, el cabecera de clúster solicita a los nodos sensores enviar el código patrón correspondiente a los datos sensados, si recibe el mismo código de varios nodos, sólo a uno de ellos se le permite enviar los datos al cabecera de clúster. Cam et al [92] introdujeron también otro esquema SDDA (*Secure Differential Data Aggregation*) basado en códigos patrones, para evitar la transmisión de datos redundantes mediante los esquemas siguientes: 1- Se transmiten los datos diferenciales en lugar de los datos brutos. 2- Se realiza la agregación de datos sobre códigos patrones que representan las principales características de los datos obtenidos. 3- Se emplea un protocolo de sleep para coordinar la activación de unidades sensoras tal que únicamente el nodo sensor se activa y recopila datos en un determinado momento.

Du et al [86] propusieron una agregación de datos WDA (*Witness-based Data Aggregation*) que asegura la validación de los nodos de fusión de datos a la EB.

La agregación segura de datos de texto cifrado se basa en una transformación de cifrado, un homomorfismo de privacidad (*PH - Privacy Homomorphism*) [95, 96]. El esquema (*CDA - Concealed Data Aggregation*) en [97] se basa en PH, CDA se puede utilizar para calcular la suma y el promedio en una WSN jerárquica, conociendo el número de nodos de sensores. Castelluccia et al [98] proponen (*HSC - Homomorphic Stream Cipher*) que permite la agregación eficiente de los datos cifrados.

2.4.6. Mecanismos de localización segura

Las WSN deben poder establecer y mantener las conexiones de los nodos en su alcance, y la conectividad de red de forma autónoma [99]. La localización puede ser parte del procedimiento de bootstrapping inicial, descubrimiento de sus vecinos, autenticación, determinación de su ubicación en la red, y establecimiento de rutas de comunicación. La localización puede ser directa incluyendo GPS o manual por pre-configuración [100, 101]. La mayor parte de los métodos de localización indirecta se basan en el uso de unos nodos baliza que conocen su posición y ayudan al resto de nodos a determinar su posición [100, 101]. La información de la ubicación de los nodos representa una amenaza para la privacidad, una manera de afrontarlo es despersonalizar los datos, de su fuente. En [102-105], se proponen cuatro enfoques; 1- la descentralización del almacenamiento de datos sensibles. 2- El establecimiento de un canal seguro de comunicación (mediante protocolos seguros como SPINS [83] que dificulta el espionaje y ataque activo). 3- cambiando el patrón de tráfico de datos (cambiando o insertando selectivamente algunos datos falsos en el tráfico de red). 4- explotando la movilidad de los nodos [104].

2.4.7. Sistemas de detección de intrusiones

Particularmente interesantes con los Sistemas de detección de intrusiones (*IDS – Intrusion Detection system*), que utilizan mecanismos que detección y reacción a las intrusiones. Esto se hace monitorizando patrones de actividad sospechosa fuera de un comportamiento normal y esperado [106]. Se suelen clasificar en dos tipos: 1- IDS basados en reglas, que detectan patrones conocidos de intrusiones [107, 108]. 2- IDS basados en anomalías que detectan intrusiones nuevas o desconocidas [66, 109]. Hay varias arquitecturas de detección de intrusos. 1- arquitectura autónoma (cada nodo funciona como un IDS independiente y detecta los ataques hacia él). 2- arquitectura distribuida y cooperativa (con un agente de detección en cada nodo, detectan ataques locales y cooperan para detectar intentos de intrusión). 3- arquitectura jerárquica (cada nodo cabecera de clúster se responsabiliza del enrutamiento dentro del clúster y hace

una correlación de eventos). Zhu et al [110] propusieron un esquema de autenticación intercalada *hop-by-hop* (IHOP) que garantiza que la EB detectará cualquier paquete de datos falsos inyectado cuando hay un cierto número de nodos comprometidos en una red basada en clústeres. Wang et al [111] propusieron un esquema para detectar en colaboración con los nodos vecinos, cuando un nodo está en fallo o es malicioso, si un nodo sospecha de algún vecino, solicita a los otros su opinión y en base a ella, toma decisiones. Albers et al [112] han propuesto un IDS local (LIDS) en cada nodo colaborando entre sí e intercambiando dos tipos de datos; datos de seguridad y alertas de intrusión.

2.4.8. Esquemas basados en confianza

Los esquemas basados en confianza suelen tener alta sobrecarga computacional. Pirzada y McDonald [113] han propuesto un enfoque para construir relaciones de confianza entre nodos a través del monitoreo pasivo de los paquetes recibidos y transmitidos que se denominan eventos. A estos eventos se les asigna un peso que se usa para calcular el nivel de confianza de un nodo. Estos valores de confianza se utilizan para el cálculo de rutas, utilizando así los nodos dignos de confianza. En [114], se han descrito métodos de búsqueda de caminos en un paradigma de computación de igual a igual. Yen et al [115] propusieron una seguridad basada en un marco de confianza. Cada nodo evalúa la confianza de sus vecinos en base a la experiencia, valor de datos, resultados de detección de intrusos, y recomendaciones de los otros. Ren et al [116] han presentado una técnica para establecer relaciones de confianza entre los nodos, basados en una solución probabilística sobre un modelo de confianza distribuida. Ganeriwal y Srivastava [117] han propuesto un marco basado en la reputación para WSN de alta integridad. Tanachaiwiwat et al [118] han propuesto un mecanismo de aislamiento de nodos de conducta inapropiada y enrutamiento basado en la confianza, si ésta está por debajo de un umbral, el nodo se considera inseguro y se evita en el enrutamiento. En [119], los autores han propuesto un modelo de confianza personalizado denominado PET, un modelo de análisis e inferencia integral de confianza para la agregación de las votaciones recibidas de los nodos de sensores.

2.4.9. Mecanismos y defensas contra algunos ataques

Ataques de denegación de servicio (DoS), cuando se transmite una señal de alta energía para interferir la comunicación de la red. [53], [106]. Estos ataques son

muy dañinos, por lo que se verán algunos mecanismos. Las defensas en la capa física se basan en la transmisión de señales cambiando rápidamente la portadora entre multitud de canales, utilizando una secuencia pseudo-aleatoria conocida por el transmisor y el receptor. El código de ensanchamiento es otra técnica para la defensa contra el *jamming*, pero requiere un diseño más complejo, un enfoque es identificar la parte atacada de la red y evitarla mediante enrutamiento Wood y Stankovic [106]. En la capa de enlace, un mecanismo contra los ataques de colisión es el uso de códigos de corrección de errores [106] que añaden procesamiento y comunicación, aunque una posible solución contra el ataque de agotamiento de la energía (*energy exhaustion attack*) es limitar la velocidad de control de admisión MAC. Otra solución, es utilizar multiplexación por división de tiempo asignando a cada nodo, una ranura de tiempo en la que puede transmitir, o también usar pequeñas tramas para reducir el tiempo disponible para capturar el canal de comunicación.

Para defenderse de los ataques DoS en la capa de transporte, Aura et al [120] han propuesto un mecanismo mediante el que cada cliente que se conecta debe demostrar su compromiso con la conexión mediante la resolución de un rompecabezas.

Ataques de suplantación de identidad y alteración. En la capa de red, una contramedida contra la suplantación de identidad y alteración es añadir un código de autenticación de mensajes (MAC) después del mensaje.

Ataque de repetición de información. Contra el ataque de repetición de información se pueden introducir unos contadores o sellos de tiempo en los mensajes.

Ataque de reenvío selectivo. Contra el ataque de reenvío selectivo se utilizan varias rutas para enviar datos [79], considerando al nodo malicioso como si hubiera fallado y buscar una ruta alternativa.

Ataques wormholes. Hu et al [121] han propuesto el mecanismo llamado cadena de paquetes para la detección y defensa contra los ataques de agujero de gusano (*wormholes*) en que un nodo malicioso escucha a escondidas una serie de paquetes, y luego establece túneles a través de una ruta de acceso en la red, y los reproduce [79]. Hu et al [122] también han presentado otro mecanismo que emplea antenas direccionales para combatir el ataque wormhole. Wang y Bhargava [123] han utilizado un enfoque de visualización para detectar agujeros de gusano en una WSN.

Ataque de desincronización, contra este ataque en la capa de transporte se obliga a cumplir el requisito obligatorio de la autenticación de todos los paquetes transmitidos entre nodos [106].

*Ataques físicos. L*a protección contra posibles ataques físicos, puede requerir nodos sensores equipados con hardware especial [106, 124-126], que al detectar que es atacado se suicide, destruyendo todos los datos y claves almacenadas en su memoria. Deng et al [127] han propuesto varios enfoques para la protección de sensores, Sastry et al [128] presentaron el protocolo ECHO basado en las propiedades físicas del sonido y la propagación de la señal de RF de los nodos sensores. En [129] se presentan mecanismos de defensa frente ataques físicos basados en búsquedas con dos fases. 1- Los sensores detectan el atacante y lo notifican a la red. 2- Los sensores reciben la notificación y programan sus estados cambiando de modo. Seshadri et al [130] propusieron un mecanismo llamado SWATT, para detectar un cambio repentino y abrupto en los contenidos de la memoria de un nodo sensor (posible ataque físico).

Mecanismos para asegurar que sólo los miembros legítimos del grupo reciban la multidifusión y difusión. Se han realizado varios esquemas de gestión de claves; los protocolos de gestión claves centralizado (utiliza una autoridad central para mantener el grupo), descentralizados (dividen la tarea de gestión de grupos entre varios nodos), y distribuidos (la actividad de gestión de claves se distribuye entre un conjunto de nodos en lugar de en un único nodo) [131]. Una forma eficiente de distribuir las claves en una red, es utilizar un árbol lógico de claves, ya que centraliza los protocolos de gestión de claves [61, 132, 133]. Di Pietro et al [61] propusieron un mecanismo de multidifusión basada en la difusión dirigida para WSN que utiliza una jerarquía lógica de claves. La difusión dirigida es una técnica de difusión de datos de alta eficiencia energética para WSN [134]. Una consulta se transforma en un interés que se difunde en toda la red. El nodo de origen comienza la recogida de datos de la red basado en el interés propagado, y los datos recogidos se envían de vuelta a la fuente por el camino inverso de la propagación de interés. Kaya et al [135] discuten el problema de la gestión del grupo de multidifusión y proponen que los nodos en la red se agrupen en función de su ubicación y se construye un árbol de seguridad sobre estos grupos. Lazos y Poovendran [132] presentaron otro esquema de distribución de claves basado en árbol, similar al basado en difusión directa propuesta por Di Pietro et al. que construye un árbol de ruta inteligente como un esquema que aprovecha la información de enrutamiento para construir la jerarquía de claves, y es muy eficiente en energía.

En [133], los autores proponen un mecanismo que utiliza la información de ubicación geográfica para construir una jerarquía lógica de claves para la multidifusión segura. En base a la información de clúster, la jerarquía de claves se construye de manera similar al propuesto en [132].

Mecanismos para el control de acceso. Duri et al [136] han propuesto un marco para proteger la información de sensores, Snekkenes et al [137] para el control de acceso basado en parámetros como el momento de la solicitud, la ubicación, velocidad, y la identidad del objeto localizado. Myles et al [138] describen la arquitectura de un servidor centralizado que controla el acceso mediante módulos de validación. Hengarter y Steenkiste [139] presentaron un marco de diseño de un mecanismo de control de acceso lo suficientemente flexible como para ser desplegado en diferentes entornos.

Protocolos de enrutamiento basado en la inundación, Ozturk et al [140] estudiaron los tipos de protocolos de enrutamiento basados en la inundación: las inundaciones básicas (cada nodo envía un mensaje de una sola vez, y ningún nodo retransmite mensajes que ya haya transmitido). Las inundaciones probabilísticas (Sólo un conjunto de nodos participa en la expedición de datos, los demás descartan los mensajes que reciben). Las inundaciones con mensajes falsos. Propusieron la estrategia de la inundación fantasma, que atrae a un atacante hacia una fuente falsa (la fuente fantasma).

También se hay disponible gran variedad de mecanismos de defensa como los aportados por Deng, Han y Mishra [141], que se orientaron a defender la EB contra los ataques físicos mediante la ocultación de su ubicación. Así como los aportados o referenciados por Dener [142], Fatema y Brad [143], Maw et al. [144], Kumari y Shukla [145], Shukla y Kumari [146], Malik [147], Kuthadi, Rajendra y Rajalakshmi [148], Karlof y Wagner [149] y otros muchos.

2.5. Conclusiones

2.5.1. Conclusiones del marco de negocio o promotor

Las empresas y suministradores de equipos y redes son muy activos en cuanto a idear nuevos servicios y aumentar su catálogo comercial. Esto implica, que la innovación, apoyada por los avances tecnológicos, es muy activa y rápida. Sin

embargo, el ámbito legislativo necesita consensuar derechos y libertades para poder legislar, por lo que no avanza a la misma velocidad que las otras áreas. Se muestra evidente la existencia de una falta de sincronía que puede provocar riesgos e inseguridades jurídicas, pudiéndose encontrar ante situaciones cuyo marco legal no se adapta o no es suficientemente concreto. Los principales perjudicados son los usuarios y las empresas, con impactos imprevisibles. Minimizar este riesgo contribuiría a disminuir los posibles costes asociados a las reclamaciones, quejas, pleitos, sanciones y deterioro de la imagen de marca. La capacidad de poder ofrecer garantía de privacidad y ganar la confianza a los usuarios, transformaría esta amenaza en una oportunidad.

En el marco de esta tesis, los servicios de IoT son prestados por redes de baja capacidad, y se necesita proporcionar una seguridad y privacidad a medida para implementar las protecciones adecuadas con el mínimo consumo de recursos, para no penalizar la calidad de servicio.

Actualmente las soluciones de privacidad las deciden y las aplican los expertos en seguridad, que inevitablemente tienen factores influyentes, como son los recursos de conocimiento, del coste de las medidas, el *time to market*, etc.

Por otra parte las soluciones de privacidad se diseñan e implementan por igual para toda la aplicación, pero el nivel de seguridad puede depender del usuario y de su marco legal asociado, teniendo esto en cuenta, puede representar un ahorro de costes.

2.5.2. Conclusiones del marco jurídico

Actualmente, la legislación sobre los datos personales no contempla los nuevos riesgos relacionados con la IoT.

Los dispositivos, productos y servicios de IoT, suelen ser susceptibles de usos y de utilidades diversas, pudiéndose utilizar en entornos y modos muy variados. Esto podría provocar la pérdida del control por parte de los fabricantes, de los distribuidores, de los proveedores de servicios y de los reguladores o legisladores. Por lo tanto, la privacidad no solo debería estar orientada a los dispositivos, productos o servicios, sino a su modo de utilización. Esto es, si cambia la utilidad del servicio, probablemente cambie el marco legislativo asociado y por consiguiente el usuario podría quedar desprotegido. Para las empresas representaría otro riesgo más, y la acumulación de riesgos podría hacer ruinoso el hecho de desarrollar estos nuevos

productos y servicios. Esta situación requiere buscar soluciones y habilitar una gestión robusta y garante para todos los agentes involucrados. En el desarrollo de la tesis se demuestra que un mismo desarrollo tecnológico, puede estar sometido a diferentes legislaciones dependiendo de quién lo utilice, cómo se utilice y para qué se utilice. Es decir, el marco legislativo va ligado a la utilización del servicio.

Las personas en sí mismas podrían considerarse como sensores que aportan datos sobre sí mismos (*Smartphone*,..). Los agentes implicados en los servicios de IoT reconocen la necesidad de tener una estandarización que permita reutilizar la experiencia y ofrecer al usuario multitud de servicios a partir de la información recogida por una gran variedad de fuentes. Será fundamental engranar los intereses empresariales con los de los usuarios. La colisión de intereses debe ser resuelta en base a la legislación vigente, por lo tanto, la participación de las áreas de negocio, jurídica y tecnológica tendría muchos beneficios.

2.5.3. Conclusiones del marco de las tecnologías

En la literatura técnica, como se ha podido observar a lo largo del capítulo, hay una gran cantidad de métodos y esquemas de seguridad y privacidad aplicables a una gran variedad de tipos de redes y situaciones. Actualmente se siguen publicando más mecanismos novedosos. Este conocimiento, ya por sí solo, requiere una base de conocimiento para poder ser gestionado y adecuadamente utilizado.

Por otra parte, es importante poder gestionar eficientemente, las actualizaciones o adaptaciones a los niveles de seguridad y privacidad que se necesiten, ante cambios sobrevenidos.

También es necesario posibilitar la realización de evaluaciones de rendimiento e impacto de la eficiencia y eficacia de las medidas de privacidad para dar realimentación adecuada a cada uno de los tres actores implicados.

3 Sistema de protección de datos personales para Internet de las Cosas

3.1. Introducción al modelo

Como se expuso en las conclusiones del estudio del estado del arte, la des-sincronía entre el área jurídica, tecnológica y comercial, provoca la percepción general de que la legislación va por detrás de las novedades tecnológicas y de las acciones comerciales que se realizan sobre ellas. Una manera de sincronizarlas, es impulsar la estrecha colaboración entre dichas áreas, posibilitando que puedan participar activamente en el diseño y desarrollo de los servicios de IoT.

Esta participación se materializaría en una participación coherente en el proceso, de forma que cuando una empresa quiere promocionar y desarrollar un nuevo servicio para los usuarios, el promotor realice la definición del servicio, ya que es quien tiene conciencia clara las necesidades y por tanto quien puede redactar las especificaciones iniciales del servicio final. Una vez especificado el servicio por parte del promotor, el área jurídica analizaría el servicio y “decidiría” los imperativos legales de privacidad, que el servicio final debe tener sobre los elementos de información que deben ser protegidos legalmente. Conocidas tanto las especificaciones del servicio como los imperativos legales, el área técnica ya podría desarrollar el servicio final, incluyendo y equipando todas las garantías legales, tanto para los usuarios como para la empresa.

Este proceso participativo permite al área jurídica poder emitir una certificación oficial de confianza de que el servicio de IoT cumple la legislación vigente (ya que las protecciones han sido definidas por esta área). Este proceso tendría la capacidad de ofrecer a los usuarios y a las empresas la garantía de privacidad que permitiera desarrollar relaciones de confianza, disminuyendo así o eliminando la percepción de inseguridad jurídica.

El área promotora o empresarial debe validar que los costes son asumibles y debe realizar un control de viabilidad del servicio, previo al desarrollo e implantación de las soluciones. El proceso también debería de armarse de tal forma que tuviera la capacidad de cumplir el time-to-market necesario. Por otra parte el área jurídica debe de validar la bondad del cumplimiento de la legislación en el funcionamiento del servicio, mediante la retroalimentación necesaria (por ejemplo la información necesaria para poder valorar el grado de cumplimiento de la legislación en materia de protección de datos personales en el servicio prestado por una ciudad inteligente).

Esta solución también debe contemplar la posibilidad de que los productos y servicios de IoT, puedan ser revendidos, o reutilizados. Este cambio de modo de uso puede implicar que la garantía de protección emitida inicialmente (cuando se diseñó el servicio), deje de ser válida puesto que el nuevo caso de uso, podría estar sometido a otro marco legal distinto o más restrictivo.

El modelo que se describe busca establecer una “Seguridad a Medida” del servicio final que se presta, proporcionando la cobertura suficiente para dar solución a los imperativos legales de privacidad. El objetivo es seleccionar los mecanismos y contramedidas de seguridad y privacidad adecuadas para implementarlas.

Se propone un sistema experto capaz gestionar la colaboración y la participación en el proceso de desarrollo de servicios de las áreas empresarial, jurídica y tecnológica para proteger la privacidad del usuario. Esta colaboración y participación se materializa en la aportación del conocimiento útil necesario por parte de cada una de las áreas implicadas. En base a este conocimiento, se efectúa la selección de soluciones.

Por otra parte la flexibilidad del sistema experto debe ser suficiente para no obstaculizar la evolución independiente de las herramientas y sistemas de cada una de las áreas mencionadas. Hay que tener en cuenta que cada una de ellas tiene su propia hoja de ruta, acorde con sus propias capacidades y planes presupuestarios para efectuar la evolución de sus sistemas y Tecnologías de la Información. Para este sistema, las únicas adaptaciones que se necesitan son el mantenimiento de los formatos en la transferencia de información; todas las demás acciones se pueden realizar por cada una de las áreas con sus propios recursos y herramientas habituales de trabajo.

La primera versión del sistema experto fue presentada en "*IEEE 1st Intech Conference*" [2], conferencia internacional que se realizó en Londres en verano de 2013. Esta primera versión se diseñó para seleccionar el nivel de seguridad y privacidad necesario para un determinado “caso de uso” de un servicio específico. El ensayo se realizó sobre cuatro casos de uso utilizando exactamente el mismo servicio (se expondrá junto con otros casos en el capítulo 4).

La segunda versión fue diseñada en 2014, incrementando sus funcionalidades, de forma que pudiera trabajar con más de una WSN, con diferentes tecnologías y diferentes servicios de IoT [3], es decir, se modificó para poder gestionar los requisitos de diversos servicios, teniendo en cuenta las posibilidades de las diferentes

tecnologías. Se estudió la mejor manera de dar privacidad a los servicios que se confeccionan a partir de la combinación de otros ya existentes. Es importante considerar que el nivel de privacidad del servicio combinado, puede diferir del nivel de privacidad de los servicios que lo componen. También se debe tener en cuenta que un nuevo servicio que se integra en un ecosistema de servicios (como puede ser una ciudad inteligente), puede abrir nuevas vulnerabilidades para todo el conjunto. Respecto a los posibles cambios del marco legal sobre los servicios finales que ya estén operativos, se tiene en cuenta la posibilidad de que se impongan nuevos niveles privacidad, como consecuencia de posibles cambios legislativos o bien por cambios estados de alarma o emergencia en una ciudad.

Esta tesis no pretende proponer ningún marco legislativo nuevo, ni ningún nuevo mecanismo de seguridad. Lo que describe es un método para seleccionar y aplicar, las soluciones de seguridad aplicando los conocimientos útiles aportados al sistema experto, por expertos humanos de cada una de las áreas de negocio, jurídica y tecnológica, colaborando en un entorno común que lo canalice.

3.2. Descripción del modelo

El sistema experto para protección de datos personales, adaptado para los productos y servicios de Internet de las Cosas, "*Personal Data Protection System for Internet of Things (PDPS-IoT)"* decide la política de seguridad y privacidad que se ha de aplicar a un cierto servicio. Tiene como entrada las especificaciones del servicio realizadas por la entidad promotora del servicio, junto con los datos personales involucrados, obteniéndose como salida la política de seguridad y privacidad (nivel de seguridad) que se debe aplicar al servicio.

El sistema permite la colaboración entre las tres áreas dividiendo el sistema experto completo en tres sistemas expertos parciales, uno para cada área participante mediante el cual canaliza el conocimiento que aporta. Estos componentes son, el sistema experto de negocio "*Business Expert System (BES)"*, el sistema experto legal "*Legal Expert System (LES)"*, y el sistema experto de soluciones tecnológicas "*Technological Solution Expert System (TSES)*". En adelante se emplearán las abreviaturas BES, LES y TSES. Entre los tres sistemas expertos se establece el flujo de la información necesaria para realizar el procesamiento y obtener los resultados necesarios para la siguiente etapa. En la figura 1 (respetando el idioma original) se muestran los bloques de información y conocimiento involucrados.

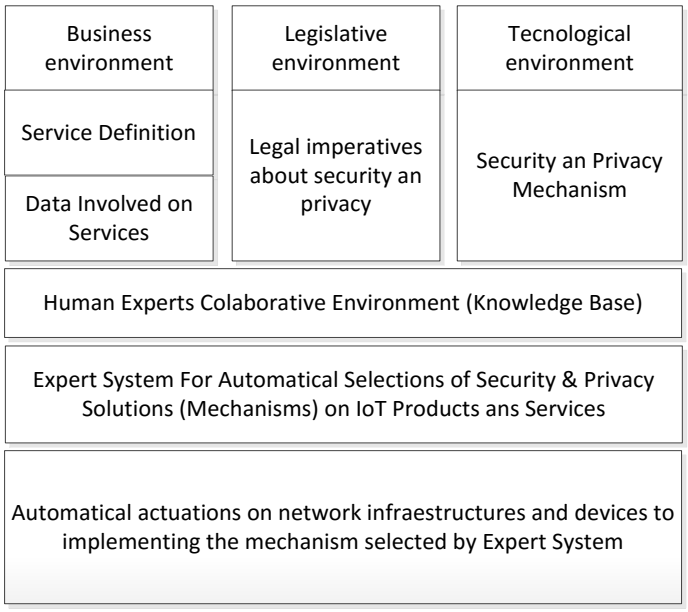


Figura 1. Información involucrada en el sistema.

El entorno de negocio BES, aporta el conocimiento relativo a la definición del servicio y los datos que éste gestiona y maneja. El entorno legal, realiza un análisis de la información que recibe de BES y LES aporta los imperativos legales de seguridad y privacidad para el servicio. El entorno tecnológico TSES aporta una base de los mecanismos de seguridad y privacidad disponibles para ser utilizados. Todo este conocimiento forma la base común de conocimientos del sistema, cuya finalidad es seleccionar las soluciones de seguridad y protección de datos.

Por último se comunican los resultados a la plataforma mediadora de servicios con la WSN para generar las actuaciones necesarias e implementar los mecanismos técnicos en la red (estas plataformas se tratarán en el siguiente capítulo, como parte del entorno de validación).

El flujo de información se representa en el diagrama conceptual de bloques del sistema PDPS-IoT que se muestra en la figura 2, donde se pueden apreciar tanto los bloques, como la conexión entre ellos. A continuación se describe la interrelación entre las partes y se menciona el contenido de los bloques de información, estos bloques de información se describirán posteriormente.

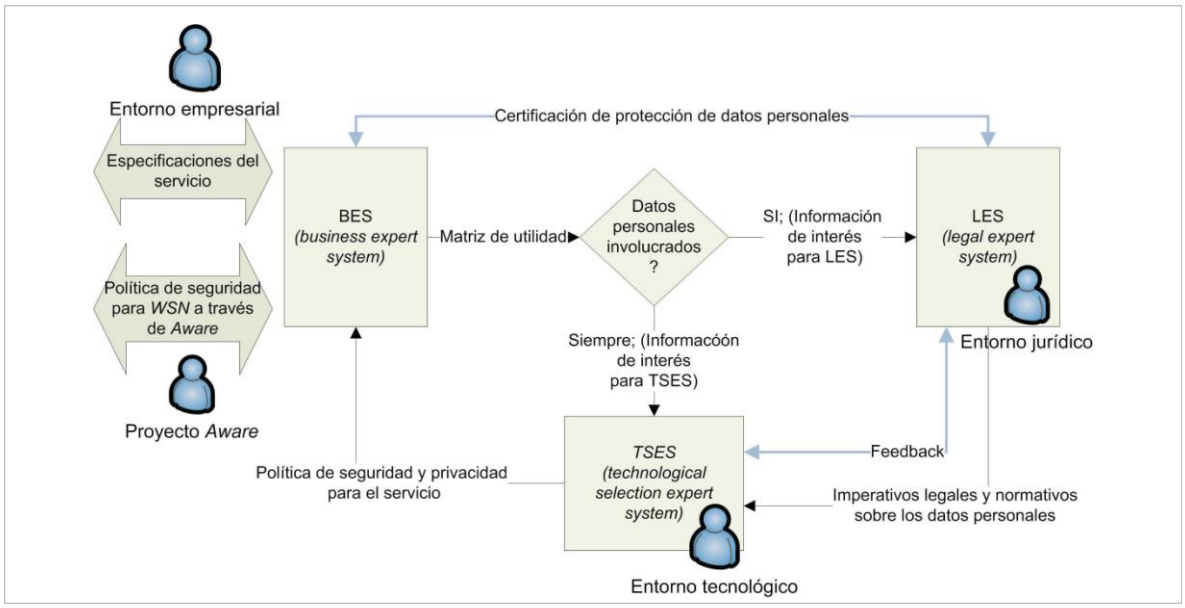


Figura 2. Sistema de protección de datos personales (PSPS-IOT).

Como se aprecia, la entrada al sistema experto es la información que procede del entorno empresarial que promueve el servicio. Esta información se almacena en BES, esta información trata sobre lo que se desea que sea el servicio. Una vez que se ha recopilado del promotor toda la información necesaria, BES compone la *"Matriz de Utilidad"* del servicio que se describirá en detalle posteriormente, es un contenedor que almacena la información relevante necesaria para el posterior tratamiento por parte del sistema. En caso de que la "Matriz de Utilidad" indique que puede haber información personal involucrada, se continuaría con el procesamiento en LES. Con la información de la Matriz de Utilidad (MU en adelante), LES seleccionaría el marco jurídico que afecta al servicio, ofreciendo a su salida el conjunto de imperativos legales que deben de aplicarse. Estos imperativos legales, son recibidos por TSES, y en base a ellos y con información sobre la tecnología que se va a utilizar procedente de la MU, TSES es capaz de adaptar los imperativos a las posibilidades de la tecnología, seleccionando los mecanismos y contramedidas de seguridad y privacidad que se deben implementar en la WSN.

Las etapas del procesamiento del sistema se esquematizan en la figura 3, donde se representan las entradas y las salidas de cada etapa de procesamiento, en la parte central se hace referencia a las bases de conocimiento utilizadas, y las salidas realimentan las entradas de la etapa siguiente.

ENTRADA	BASE DE CONOCIMIENTO	SALIDA
Requisitos del servicio (BES)	Empresarial (sobre el servicio) (BES)	Matriz de utilidad Datos Personales (LES)
Matriz de utilidad Datos Personales (LES)	Jurídico (sobre legislación) (LES)	Imperativos legales Datos a proteger (TSES)
Imperativos legales Datos a proteger (TSES)	Tecnológico (sobre ataques, servicios y mecanismos de seguridad) (TSES)	Políticas válidas (BES)
Políticas válidas (BES)	Empresarial (sobre variables críticas de negocio). (BES)	Decisión final (BES; LES; TSES)
Decisión final (BES; LES; TSES)	Control de validez por el ámbito Jurídico (LES)	Certificación, Registro y comunicación (LES)

Figura 3. Etapas del procesamiento

Hay que hacer notar que la clave del modelo y del procesamiento de la información es posible gracias a la formalización de la información relevante en la MU. A continuación se describe en detalle el funcionamiento de cada una las partes del modelo.

3.2.1. Sistema experto de negocio (BES)

El sistema experto BES (*Business Expert System*) es la parte de PDPS-IoT que canaliza el conocimiento de la especificación del servicio final que realiza el promotor del servicio, esta información alimenta a la base de conocimiento de BES y se compone de la información del “Servicio”, de los “datos” que podrían ser sensibles (BES aún no puede estar seguro de que lo sean), y finalmente las características técnicas del tipo de red que tiene pensado utilizar el promotor para prestar este servicio de IoT. Esta información recopilada del promotor se almacena en la base de conocimiento de BES y en base a su contenido se confecciona la "*Matriz de Utilidad*". La MU se compone de dos partes.

La primera parte contiene información sobre el propio servicio, sobre sus requisitos, sus actores, sobre las personas monitorizadas y sobre los datos que se van a gestionar en el servicio final en cuestión. En esta primera parte de la Matriz de Utilidad se encuentra la información que necesita el sistema experto legal LES, para poder obtener el marco legal que afecta al servicio y seleccionar los imperativos legales. En la tabla 2 se enumera la información más importante que maneja esta

primera parte de la Matriz de Utilidad. Cada uno de los conceptos que aparecen en la tabla tiene un conjunto de valores catalogados para ofrecer al promotor un conjunto de formularios guiados con desplegables, para disminuir el nº de oportunidades de error al rellenarlos.

INFORMACIÓN RELEVANTE PARA OBTENER EL MARCO LEGISLATIVO
Del servicio: Nombre del Servicio; Tipo Servicio; Tipo Entorno; País
De los actores: Promotores; Usuarios; Monitorizados
Persona monitorizada: Tipo Persona; Capacidad Legal; Necesidades Especiales
Requisitos de Servicio: Necesaria Continuidad Del Servicio; Criticidad Del Servicio
Datos: Identidades de usuario; Identificativos; Registros; Actividad; Configuración; Información estadística; Lecturas, modificaciones, consultas y eliminación de datos de usuarios; Datos recopilados; datos del usuario para gestión; Datos técnicos propios de la red

Tabla. 2. Primera parte de la Matriz de Utilidad.

La información del servicio ofrece la información sobre el “País”, con lo que se comienza con seleccionar un ámbito legislativo general. Respecto al “Tipo de Servicio” este valor representa el tipo al que pertenece el conjunto de servicio que se va a proporcionar por ejemplo telemedicina, e-salud, teleasistencia, seguridad del hogar, video vigilancia, etc. Cada uno de estos tipos de servicio tiene un marco asociado de prestación del servicio y de tratamiento de datos que por supuesto es compatible con las leyes generales de protección de datos, pero que realizan algunos matices propios del servicio. El “tipo de entorno” actúa como un modificador del anterior, puesto que no es lo mismo la video vigilancia en un hogar, que en un ministerio, que en un centro de trabajo, en la calle o en un colegio, cada entorno tiene sus propias particularidades en cuanto a la legislación que nos ocupa.

En cuanto a la información referente a los actores, es importante saber quién es promotor del servicio, una empresa privada, un ministerio impulsando una nueva política de salud por ejemplo, o video vigilancia policial; hay promotores que tienen sus propios ámbitos de actuación y excepcionalidades en las leyes que se han de tener en cuenta. Por otra parte la consideración de usuarios del servicio, se toma en el sentido de la persona o entidad que obtiene un beneficio (social o económico) de la utilización del servicio. Por último están quienes aún estando sometidos a monitorización, pueden ser usuarios del servicio, o no serlo (por ejemplo, una persona que pasa por la calle y es grabada por una videocámara), por lo tanto también deben ser considerados los derechos de las personas que son afectadas de forma colateral.

De la multitud de entidades que pueden ser monitorizadas, un caso especial desde el punto de vista del tratamiento de datos son las personas o colectivos de

personas. En cuanto al tipo de persona que puede modificar el marco legislativo encontramos a los niños y menores de edad, a los adultos y a las personas mayores. También hay que considerar sus necesidades especiales, ya que puede haber marcos legales que se modifiquen, por ejemplo discapacidad psíquica, cognitiva etc. al igual que su capacidad legal como puede ser prisión, libertad vigilada, órdenes restrictivas de algún derecho o libertad, etc.

En lo que respecta a los requisitos del servicio, también podrían tener implicaciones legales ya que se refiere a la “necesidad de Continuidad del Servicio” que dependiendo del servicio de que se trate puede tener mucho impacto; la “Criticidad del Servicio” también es importante por el impacto que puede provocar una disfunción del mismo, en cualquier caso aunque no modifiquen o complementen el marco legislativo del servicio, estos dos parámetros son imprescindibles para la segunda parte de la MU, porque TSES lo necesita.

Los Datos personales susceptibles de ser protegidos por la ley son aquellos que en base a su conocimiento o divulgación pueden provocar algún grado de discriminación, en el caso español se clasifican en tres niveles de protección, el nivel mínimo o básico lo componen los datos de identificación, educación, profesión, laborales, y demás información de este tipo. El nivel intermedio lo componen los datos referentes a la solvencia económica, datos financieros, multas administrativas y penales así como, datos fiscales, sobre impuestos etc. y por último entre los datos de nivel máximo están los de origen racial, salud y vida sexual, creencias religiosas, ideología política, afiliación y sindicación o similares.

La segunda parte de la MU contiene la información sobre el tipo de red elegida para prestar el servicio, sobre los recursos de los nodos sensores y de la estación base, los tipos de conexión y comunicación que se utilizan, la topología de la red, el tipo de encaminamiento, señalización, sincronismo, en esta parte de la MU es clave saber si la continuidad del servicio es o no un requisito, el nivel de criticidad del servicio (crítico para las personas, para las infraestructuras, etc.). Estos datos de la Matriz de Utilidad son los que TSES necesita junto con los imperativos de seguridad. Cada uno de los conceptos que aparecen en la tabla 3 tiene un conjunto de valores catalogados para dar al promotor un conjunto de formularios guiados con desplegables, para disminuir el número de oportunidades de error.

INFORMACIÓN RELEVANTE PARA OBTENER LAS SOLUCIONES TECNOLÓGICAS
Tipo de Red; Recursos de los Nodos Sensores; Recursos de la Estación Base; Topología de Red; Comunicación
Protecciones del servicio: Manejo de fallos; Funcionamiento en Modo autónomo
Criticidad para el servicio: De la señalización; Del sincronismo
Otros: Intervalo monitorización; Transmisión compartida; Acceso físico a los nodos; Tipo de Gestión; agregación de la información
Datos: Agregados/Desagregados; Buffers; Conexiones; Configuraciones; Datos de servicio; De nodos; De enrutamiento

Tabla. 3. Segunda parte de la Matriz de Utilidad

También se añaden observaciones para que el administrador pueda contemplar nuevos casos o depurar los formularios y sus opciones.

3.2.2. Sistema experto jurídico (LES)

Este sistema se ha inspirado en los sistemas expertos jurídicos descritos por la Doctora Cuadrado Gamarra en su libro “Aplicación de los Sistemas Expertos al Campo del Derecho” [4]. La misión de LES es reconocer el marco legislativo sobre privacidad y protección de datos adecuado al servicio, y seleccionar los imperativos legales que se deben aplicar para proteger los datos sensibles considerados por el marco legal.

LES recibe de BES los datos de la Matriz de Utilidad, que son relevantes para su finalidad y compone la plantilla de evaluación de impacto DPIA-T (*Data Protection Impact Assessment Template*) [150] en caso de que ésta no exista. En caso de que la base de conocimiento de LES tenga constancia de que ya existe una DPIA-T y ésta se ajuste a las condiciones de prestación del servicio (por ejemplo para el servicio de *Smart Grid*, ya está confeccionada y admitida oficialmente por la unión europea), se utiliza.

Se selecciona por una parte el marco legislativo que afecta al servicio y se agrupan los conjuntos de datos que son gestionados por el servicio, distinguiendo los personales y los que sólo afectan al servicio de IoT, y se aplica la normativa específica a esos conjuntos de datos, asignándoles el nivel de protección legal necesario.

La base de conocimientos jurídicos, no almacena leyes sino el conocimiento de los expertos del área, que son estructurados con la finalidad de obtener los imperativos legales y aplicarlos a los datos del servicio final que deben tener un determinado nivel de protección. Los imperativos legales se extraen del marco legal correspondiente. Con la finalidad de alcanzar un entendimiento entre el área legal y tecnológica se han nombrado los imperativos de forma que se corresponden con el

significado de los servicios de seguridad y privacidad de la recomendación X.800. Estos imperativos son los que se deben aplicar correctamente a los conjuntos de datos, y se relacionan en la tabla 4.

Imperativos	Servicio de Seguridad y privacidad
Veracidad de los actores	Autenticidad
Autorización de acceso	Control de acceso
Revelación / divulgación	Privacidad
Veracidad del contenido	Integridad
Responsabilidad Actores	No repudio
Continuidad de servicio	Disponibilidad

Tabla. 4. Relación de imperativos de seguridad.

En base a los elementos de información procedentes de la MU, se establece un mecanismo de selecciones sucesivas hasta llegar a obtener el marco legal que afecta al servicio concreto de IoT. Este marco legal seleccionado, es el que se aplica a la parte de la MU referida al conjunto de datos gestionado por el servicio, una vez que se han identificado los datos que necesitan ser protegidos (los datos que identifican a personas concretas, así como los que relacionan a la persona con sus datos recopilados, procesados o históricos, eventos que identifiquen su estado o situación, etc.).

Generalmente un servicio de este tipo está formado por sensores que recopilan datos, estos datos pueden estar ligados al usuario del que se recopilan. Respecto a la gestión del servicio se dan altas de usuarios con sus datos de filiación, etc. que también pueden necesitar de protección. Por otra parte, un atacante contra los datos técnicos de la red podría descubrir o inferir información sensible del cliente como podría ser los datos de su ubicación.

Una vez que se dispone del marco legislativo y de los conjuntos de datos que se deben proteger, el siguiente paso consiste en asignar los imperativos de seguridad y privacidad a los conjuntos de datos sensibles en base a la normativa aplicable. Cada imperativo sobre un determinado conjunto de datos se realiza en base a una normativa específica para un cierto tipo de servicio concreto.

El resultado final es que a cada conjunto de datos se le asignan una serie de imperativos de seguridad y privacidad como se muestra en la tabla 4. A cada imperativo legal le corresponde un servicio de seguridad, como se verá más adelante en el próximo apartado.

Estos resultados son coherentes con la confección de la plantilla de evaluación de impacto DPIA-T como muestra la tabla 5, que representa un ejemplo de entrada a TSES. La razón de unificar los resultados con formato DPIA-T es que cuando se integran nuevos servicios en un ambiente holístico, normalmente se necesita reajustar la privacidad de los servicios colaterales, para así evitar los ataques sobre las nuevas vulnerabilidades que pudieran aparecer. Esto fuerza a revisar servicio por servicio y también todo el servicio conjunto. Como resultado de este proceso algunos mecanismos y contramedidas podrían ser modificados o ajustados.

DPIA-T : "*Nombre del servicio de IoT*"	
Imperativo	**Objetivo del ataque (Datos)**
Veracidad de los actores	Suplantación
Veracidad del contenido	Falsear el contenido de la información monitorizada.
Revelación / divulgación	Espiar los datos de monitorización Enlazar los datos monitorizados con su propietario. Suplantar a los elementos del servicio.
.....	……..

Tabla. 5. Relación los imperativos y los objetivos de los ataques.

3.2.3. Sistema experto tecnológico (TSES)

La base de conocimientos de TSES almacena el conocimiento útil sobre los servicios y mecanismos de seguridad, se trata de que éstos estén lo más actualizados posibles con las últimas novedades. Por otra parte estos mecanismos se adecúan mejor a ciertos tipos de red que a otros. Manteniendo un catálogo de tipos de redes WSN y relacionándolos con los mecanismos más apropiados, es posible seleccionar las mejores soluciones.

La base de conocimientos también incluye información sobre los ataques que pueden actuar contra los imperativos de seguridad y privacidad impuestos por LES, Estos ataques se relacionan con los mecanismos y contramedidas que los afrontan.

TSES recibe los imperativos legales sobre los conjuntos de datos que se deben proteger, se transforma esta información en servicios de seguridad y privacidad concretos, y capturando aquellos ataques que pueden actuar sobre estos servicios de seguridad y privacidad, se seleccionan los mecanismos y contramedidas más adecuadas para proteger estos datos en este tipo de red y para este servicio.

Estos datos están expuestos a una serie de amenazas en un determinado tipo de red, afortunadamente (según se pudo comprobar en el estado del arte) estos ataques disponen de una gran variedad de contramedidas y soluciones muy efectivas

y eficientes debido a la gran actividad investigadora en este campo. Como resultado de esta actividad, es posible cubrir la mayoría de los casos que se presentan habitualmente, aunque muchos de ellos deben ser adaptados. En caso de no encontrarse suficientes mecanismos para dar solución a un determinado caso, el sistema generaría una "alarma de cobertura de conocimiento", esta alarma (*warning*) insta a los expertos correspondientes a resolver el problema.

Como se vio anteriormente, la Base de conocimientos tecnológicos, establece una relación conceptual directa entre los imperativos legales obtenidos de LES y los servicios de seguridad de la Recomendación X.800 [18] en TSES (tabla 4). Esta información se toma como base para confeccionar la plantilla de evaluación de impacto DPIA-T, y se complementa como en la tabla 6 con un conjunto de Imperativos de seguridad y privacidad que actúan sobre el conjunto de datos que se ha de proteger en un tipo de red determinado. Con estos imperativos se obtienen los servicios de seguridad y se aplican sobre el conjunto de datos protegidos. Ahora se relacionan los ataques catalogados, sobre los servicios de seguridad que se necesitan y se seleccionan los mecanismos disponibles según el tipo de red. Entonces se obtiene una lista de mecanismos.

DPIA-T : "*Nombre del servicio de IoT*"			
Servicio de seguridad	**Ataque**	**Objetivo**	**Defensa**
Disponibilidad	DoS	1- La capa física se degrada y la comunicación entre nodos es imposibilita (*jamming*). 2- Un nodo malicioso envía sus datos a la red.	Se debe detectar la situación para afrontarla
Autenticación	Sybil	Un nodo pide múltiples IDs, si el ataque tiene éxito puede destruir el mecanismo de confianza.	Restablecer la confianza expulsando al nodo malicioso.
	Nodo clonado	Cuando la ID de un nodo es copiada y replicada en un nuevo nodo que se introduce en la red	Detectar y revocar el nodo malicioso
	Nodo falso	Introduce tráfico en la red para evitar la comunicación de los nodos legítimos (Inyectando mensajes con datos falsos, reclamando continuamente autorización, etc.).	Identificar le nodo falso descartando todos sus mensajes.
Integridad	Mensaje corrupto	Un mensaje llega al receptor con un contenido diferente al enviado por la fuente.	Asegurarse de que los mensajes no han sido alterados.
Privacidad	Eavesdropping (escucha)	Otros dispositivos escuchando en la misma frecuencia pueden interceptar las comunicaciones entre nodos.	Usar autenticación y cifrado. Anonimizar los datos.
	Captura de nodos	Un nodo es capturado y criptoanalizado (las claves secretas, ID de nodo, las políticas de seguridad, etc.	Pocos datos almacenados en los nodos y renovar las claves.

Tabla. 6. Plantilla de evaluación de impacto.

El catálogo de ataques se muestra en la tabla 7.

CATALOGO DE ATAQUES	DESCRIPCIÓN
Ataque	El nombre del ataque
Tipo de red	Cada tipo de red es sensible a ciertos ataques e inmunes a otros
Servicio de seguridad atacado	El servicio de seguridad (imperativo legal) al que vulnera.
Impacto del ataque	Cuál es el impacto que provoca (alto, medio, bajo)
Mecanismos / contramedidas	Conjunto de mecanismos que afrontan el ataque para este tipo de red.

Tabla. 7. Catálogo de ataques.

Este catálogo de ataques establece también una catalogación de mecanismos y contramedidas que son válidas para cada tipo de red según sus características. Estas características manifiestan vulnerabilidades a ciertos ataques. Estos ataques se afrontan mediante mecanismos y contramedidas para ese tipo concreto de red. Estos tipos de red de los que se está hablando son por ejemplo “la parte del hogar inteligente en la Smart Grid”, etc. Entre los datos relevantes del tipo de red, se encuentran los recursos, la conectividad, el tipo de routing, etc.

3.3. Visión conjunta del sistema

El proceso básico de selección de las políticas de seguridad y privacidad, se establece en base a la información contenida en las bases de conocimiento del sistema. Este conocimiento surge de la cooperación entre las áreas que operan con los bloques funcionales BES, LES y TSES, cuya interrelación se establece mediante la transferencia de información y resultados. Tras de numerosos ensayos y pruebas de concepto, se ha dado prioridad a la simplicidad, de tal modo que el sistema experto sea rápido y fácil de usar. Pero esto no es gratuito, la responsabilidad de la fiabilidad y la cobertura de las políticas, los mecanismos y contramedidas, se transfiere a los equipos de expertos de cada una de las tres partes, BES, LES y TSES, siendo éstos los responsables de la cobertura y fiabilidad de la información contenida en las bases de conocimiento en su ámbito.

En el ámbito empresarial, el promotor del servicio es en quien recae la responsabilidad de definir el servicio, y proporciona la información al sistema través de formularios guiados. Con esta información se construye la Matriz de Utilidad (información sobre el tipo de servicio final, y la definición de los conjunto de datos involucrados). Esta información es recibida por LES quien selecciona el marco legal y la aplica al caso en concreto y lo pone en formato DPIA-T para ser utilizado por TSES.

En la figura 4 se proporciona una visión general de la cadena de selección de los mecanismos de seguridad que constituirán la política de seguridad y privacidad.

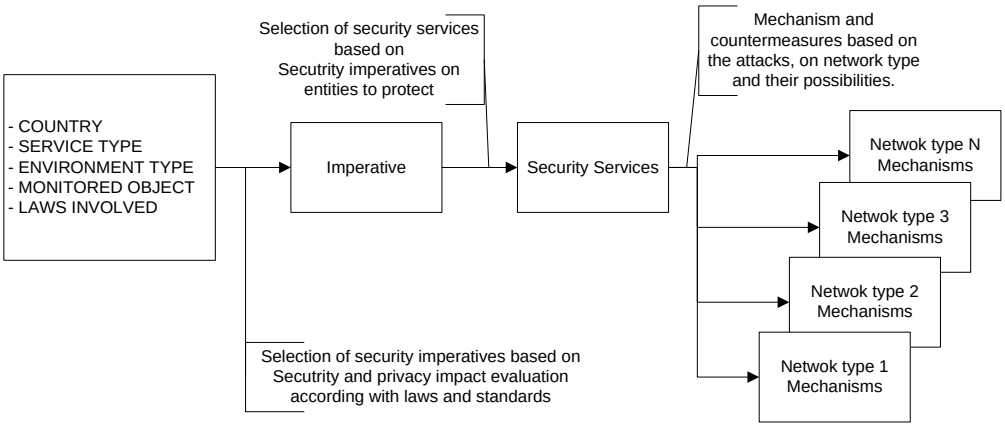


Figura 4. Cadena de selección de mecanismos de seguridad.

Por otra parte BES también provee la información técnica necesaria sobre el servicio para que TSES pueda obtener las posibles vulnerabilidades de servicio, y así saber cuáles son los mecanismos y contramedidas disponibles para ese tipo de red. Así, TSES se pone a trabajar cuando obtiene ésta información de BES, y los imperativos legales de LES.

La correcta selección de los servicios y mecanismos de seguridad en TSES, es mejor, cuanto mejor sea la información disponible sobre la tecnología, la topología y la información extraída de la Matriz de Utilidad [2,3]. Cada tecnología es capaz de soportar sólo ciertos mecanismos de seguridad y privacidad sin afectar a la calidad del servicio, el reto está en alcanzar el nivel de privacidad que se necesita con los mecanismos disponibles.

El resultado final que se obtiene es un conjunto de mecanismos y contramedidas que logren obtener el nivel de seguridad necesario. En el caso de que el sistema no sea capaz de encontrar solución para todos los requisitos de seguridad y privacidad, se lanza una advertencia (*warning*) de “insuficiencia de conocimientos”, indicando el problema encontrado y encaminado al responsable del conocimiento insuficiente.

El entramado de información se muestra en la figura 5.

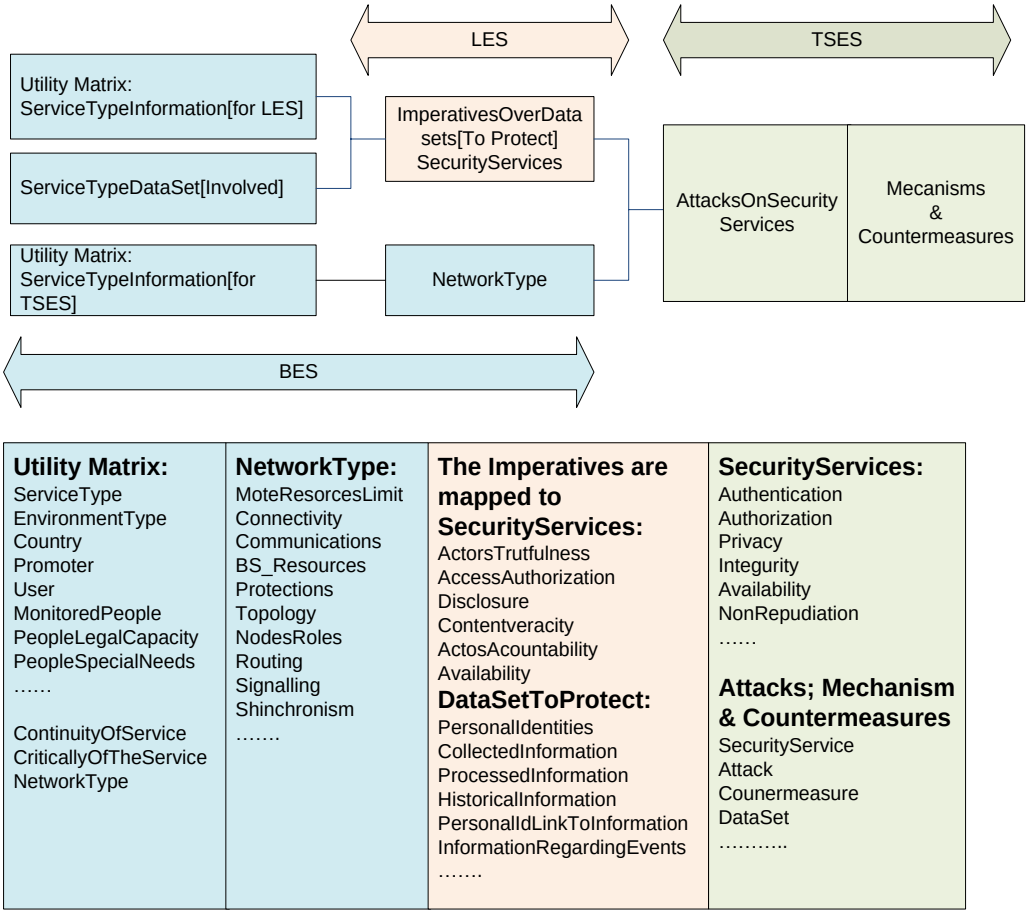


Figura 5. Información involucrada en el sistema.

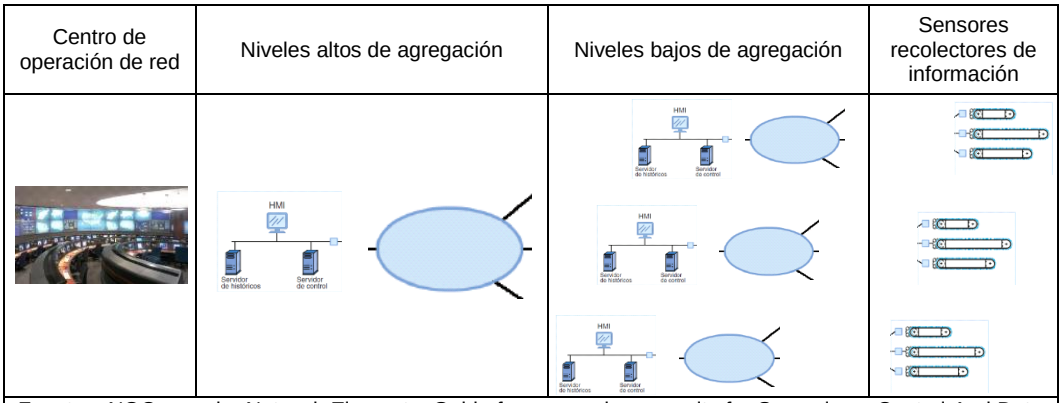
La clave para que todo el proceso funcione correctamente es el conocimiento útil que aportan los expertos de cada una de estas áreas. Pero esta tarea sería prácticamente inabordable si no se dispusieran de herramientas de ayuda al trabajo de estos expertos. La más significativa tiene como finalidad liberar al experto de la tarea repetitiva que supone el filtraje de los documentos relevantes donde se encuentra el conocimiento útil para las bases de conocimiento. Esta herramienta funciona de la siguiente manera, un experto, por ejemplo el tecnológico, accede a las bases de datos donde se encuentran los documentos científicos y extrae los artículos nuevos en formato pdf y los almacena localmente. A continuación pasa la herramienta con los criterios que le interesa sobre todos los documentos capturados y almacenados y se ordenan por relevancia. Esta aplicación previamente ha aprendido de los documentos que en anteriores ocasiones el experto ha tomado como relevantes, haciendo un tratamiento de patrones semánticos. Esta herramienta sólo se menciona puesto que todavía está en desarrollo por el grupo de investigación.

3.4. Extensión del sistema

El sistema PDPS-IoT adquiere su máxima expresión en entornos amplios como es el control de la privacidad en las *Smart Cities*. El sistema propuesto puede considerarse desde un punto de vista general, como una herramienta de toma de decisiones sobre la privacidad, su fiabilidad depende del conocimiento que contenga y de lo útil que sea éste conocimiento para afrontar los distintos casos.

Esta herramienta de toma de decisiones sobre la privacidad, podría formar parte del centro de operaciones de red *"Network Operation Centre (NOC)"*, (figura 6) que concentra la inteligencia, la gestión, la toma de decisiones, la planificación, la supervisión, la operación y el mantenimiento de las redes y los servicios de IoT (un NOC armoniza los sistemas y herramientas, de forma que aunque las actuaciones en realidad se realicen por todo el territorio, virtualmente es como si se concentraran en la misma sala, bajo un mismo paraguas). En este entorno sería posible mantener un nivel de seguridad y privacidad coherente para todo el ecosistema de servicios de IoT.

Una necesidad que podría darse (por múltiples causas), es poder disponer de la capacidad de modificar los niveles de alarma y alerta de las ciudades ante situaciones de emergencia, adaptando así las condiciones de seguridad y privacidad. En el entorno de las Smart Cities, disponiendo de los planes de seguridad y privacidad pre-configurados en función del nivel de alarma o alerta, los cambios podrían aplicarse muy eficazmente y en poco tiempo. El sistema experto tomaría la decisión y desde el NOC se desplegarían las actuaciones automáticas y manuales necesarias para realizar el cambio de estado de alarma requerido por la situación que se trate.



Fuentes. NOC, google; Network Elements, Guide for companies: security for Supervisory Control And Data Acquisition (SCADA), INTECO with sponsorship from Deloitte.

Figura 6. Centro de Operación de Red (*NOC*)

El servicio que presta una *Smart City* a sus ciudadanos depende del catálogo de servicios que integra. Desde un punto de vista holístico, este "servicio conjunto", se compone de varios servicios individuales que se asocian entre sí para aumentar la funcionalidad del conjunto. Cada uno de los servicios individuales que se integra en el ecosistema de servicios de una ciudad, debe de equiparse con los mecanismos de seguridad y privacidad para defenderse contra los ataques dirigidos a él, y contra las nuevas vulnerabilidades que aparezcan en el ecosistema debido a su integración.

El servicio conjunto de la ciudad podría verse como una superposición de los servicios individuales como se muestra en la figura 7 (respetando el idioma original), en la que algunos de los servicios inteligentes tienen una infraestructura real (nodos sensores, vías de comunicación, estación base, etc.) que llamaremos "*Real Smart Services (RSS)*", y conviven con otros servicios, que se realizan mediante la combinación y el procesamiento de la información disponible, a estos servicios los llamaremos "*Virtual Smart Services (VSS)*" [151-153]. En estos casos hay que tener en cuenta que los fallos en los datos, pueden afectarse entre sí al igual que las vulnerabilidades y los ataques. Los niveles de seguridad y privacidad de ambos deben tener un nivel coherente.

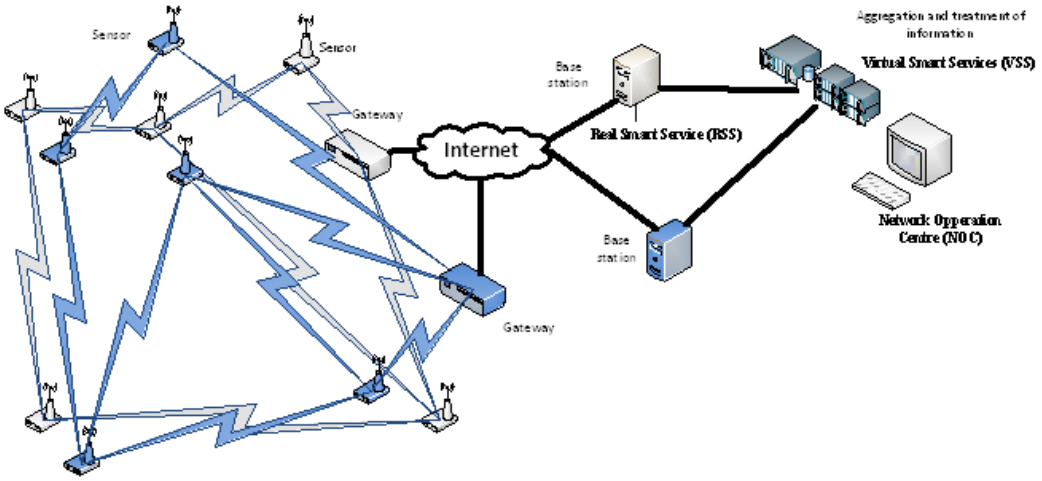


Figura 7. Servicio conjunto. Servicios compuestos.

Para poder gestionar todo esto. Es importante tener en cuenta que cada servicio particular se suele analizar mediante una plantilla de evaluación impacto (*DPIA-T Data Protection Impact Assessment Template*) [150]. En el entorno de Smart City cada servicio debe tener su propia plantilla DPIA-T, y el servicio conjunto de la ciudad debería tener el suyo, una plantilla DPIA-T para el servicio integral. En caso de añadir un nuevo servicio individual en la ciudad, se considerarían no solo la seguridad

propia, sino su impacto en toda la ciudad. Como se puede ver, la DPIA-T es una herramienta muy potente de revisión de los mecanismos de seguridad y contramedidas para satisfacer las leyes de seguridad y protección de datos. Debe estar permanentemente actualizada.

3.5. Evaluación del rendimiento

El objetivo de todo el sistema propuesto es proteger la privacidad del ciudadano en un entorno holístico de servicios, pero esta protección no solo depende que se hayan elegido buenos mecanismos de seguridad y privacidad acordes con legislación, también que los sistemas que canalizan el servicio funcionen correctamente y sean capaces de reaccionar como se espera de ellos ante los ataques. Si el área jurídica emite una certificación de garantía de privacidad, sería lógico que quisiera conocer mediante informes periódicos, el grado de protección del ciudadano, las nuevas amenazas que ocurren y su impacto. Permitiría mantener o no la garantía y conocer de primera mano los problemas, para dar posibles soluciones legales a las nuevas amenazas. Para ello se puede montar un sistema de supervisión y reporte como se verán en los siguientes apartados. En el marco de esta tesis hay tres elementos básicos que proteger así como su interactuación. La red de sensores, la plataforma de servicios y el sistema experto. En esta tesis, suponemos que tanto la plataforma de servicios como el sistema experto se protegen por los métodos habituales de seguridad informática, con su gestión habitual y sus auditorías normales, para enfocar el estudio sobre las redes de sensores.

3.5.1. Recolección de eventos

Cualquier incidencia o anomalía que ocurre en las WSN se comunica a la plataforma correspondiente para que ésta pueda tomar las acciones de operación y mantenimiento adecuadas. El interés de esta tesis se centra únicamente en los eventos provocados por las incidencias que se refieren a los ataques contra la privacidad.

Para poder realizar una evaluación, las WSN deben de ser capaces de detectar las incidencias y reportarlas a la plataforma de servicios y desde esta, al sistema experto, estos mensajes llevan un sellado de tiempo (*timestamp*). Así un mensaje recibido por el sistema experto tendrá los tiempos procedentes de la WSN, de la plataforma y el suyo propio para poder evaluar los posibles retardos en la transferencia en las notificaciones de incidencias cuyo formato es:

- Cabecera: Sellado de tiempo; id elemento; nº de secuencia
- Cuerpo: tipo de alarma/ataque; nivel de alarma; actuación realizada; volcado de memoria.
- Fin de alarma: Indicador de final del mensaje

La plataforma recibe los mensajes procedentes de las WSN, los analiza y los agrupa por orígenes y por tipo de ataque, lanzando las acciones pertinentes en su ámbito (informa al staff de seguridad para que tome acciones, etc.), Esta agrupación de alarmas la encapsula y la retransmite al sistema experto:

- Cabecera con su sellado de tiempo, el origen de la alarma, la clase de alarma.
- Cuerpo del mensaje envía todos los datos de las alarmas originales relacionadas excepto los volcados de memoria, en su lugar se transmite el código de fin de la actuación y el impacto.
- Final de mensaje: Indicador de final del mensaje

El sistema experto respecto a la operación y el mantenimiento no trabaja en tiempo real, sino solamente trabaja como un módulo de informes periódicos.

3.5.2. Indicadores clave del rendimiento

El sistema de supervisión y reporte se basa en los indicadores clave de rendimiento (*Key Performance Indicators KPI*) en adelante nos referiremos a ellos como KPI, que son las siglas más empleadas en la literatura al respecto.

La finalidad de las WSN es dar el servicio especificado, la de las plataformas es controlar los servicios y crear otros nuevos a partir de ellos si se necesita, y la finalidad del sistema experto es garantizar que se cumplen las leyes de protección de datos. La evaluación del grado de protección de la privacidad del ciudadano, se realiza respecto al cumplimiento del marco legal vigente. El sistema experto se ha de responsabilizar de ello, es decir, de dar una realimentación del grado de cumplimiento de la legislación vigente en materia de protección de datos, o nivel de cumplimiento de los imperativos legales.

Cada ataque que se produce, provoca un "impacto" determinado sobre la información que debe de protegerse, por lo tanto, el grado de cumplimiento de la legislación vigente se debe determinar en base a este “impacto” real que ha sucedido (desafortunadamente, el impacto normalmente se sabe a posteriori).

Se categorizará como "0" los ataques sin impacto registrado, con "1" los ataques con impacto sobre los datos que no están sometidos a protección legal, y con "2" los ataques que tienen impacto sobre los datos protegidos legalmente.

Con estas mediciones confeccionamos los siguientes tres indicadores:

- Ataques sin impacto legal, son los ataques de categoría (0 U 1).
- Ataques con impacto legal son los ataques pertenecientes a la categoría (2).
- Severidad de los impactos: un valor que se añade a cada ataque que ha tenido impacto, es decir las categorías 1 y 2.

A los ataques de categoría 0 se les pone severidad 0, si en el transcurso del tiempo se aprecia que en realidad sí que ha tenido impacto, se re-categoriza con la categoría y severidad que le corresponda.

Las detecciones de los ataques se pueden clasificar como muestra la tabla 8:

Tipos de detecciones de ataques		
	Positivos	**negativos**
Verdaderos	**(V+).** Se detecta un ataque y es cierto. Permite actuar con rapidez.	**(V-).** No hay detección y no hay ataque.
Falsos)	**(F+)** Se detecta un falso ataque. Genera actuaciones contra ataques irreales.	**(F-).** No hay detección, pero hay un ataque No se actúa hasta que se detecta por otros medios.

Tabla. 8. Detección de ataques

Se producen impactos reales cuando se detectan como verdaderos positivos, como falsos negativos y posiblemente por reacciones negativas provocadas por las actuaciones frente a los falsos positivos detectados. Por lo tanto el estudio de impacto debe centrarse en las causas que producen los [V+, F-, F+], en base a este estudio se deben componer los informes pertinentes para las áreas correspondientes.

En la tabla 9 se muestra la correspondencia existente entre las detecciones y sus impactos.

Ataques vs Tipos de detecciones de ataques			Destino del informe
Categoría	**Detección**	**Impacto en la información**	
0	**F+, V-**	Cuando no se ha producido impacto alguno.	Útiles para que el área tecnológica mejore la detección de F+.
1	**V+, F-, F+**	Cuando el impacto no vulnera la legalidad-	Útiles para las áreas de negocio y tecnológica.
2		Cuando el impacto vulnera la legalidad.	Útiles para el área jurídica. Las demás áreas deben conocerlo.

Tabla. 9. Categorización de los ataques.

Cuando las WSN detectan alguna incidencia respecto a la privacidad recogen el evento e informan al NOC de lo que ocurre. Estos indicadores pueden agregarse para ofrecer una visión del servicio en general o bien desagregarse para dar detalle de los servicios individuales con valores: $V_{n', k'}$ (valor del indicador k', para el servicio n'). Cuando se habla de impacto se refiere a un valor k' ∈ [1, k] dependiendo del servicio específico n' ∈ [1, n] que ha sido agregado. El valor V corresponde al valor del impacto.

De esta manera se pueden conocer el número de ataques sin impacto legal, el número de ataques con impacto legal y una medida cuantitativa de la gravedad o severidad de los impactos. También es posible saber cuáles son los servicios más atacados, los ataques que causan mayor impacto, y por lo tanto evaluar los mecanismos contra los ataques.

Para encontrar las causas principales de los impactos no deseados, se deben obtener medidas auxiliares para establecer un plan de mejora. Estas medidas se obtienen de las plataformas de servicios que bien pueden enviarlas, o bien que permiten acceder periódicamente y procesar esta información de sus log. Estos indicadores son básicamente dos:

1- Efectividad de los mecanismos y contramedidas contra los ataques a la seguridad
2- Sobrecarga introducida por los mecanismos, al sistema cuando éstos actúan y puedan afectar a la calidad del servicio (tráfico, retrasos, y consumo excesivo de recursos), es decir, por sobrecarga causada en la realización de acciones defensivas.

La <u>efectividad</u> de los mecanismos y contramedidas se evalúa por el nº de veces que ha tenido que actuar y sobre el resultado de sus actuaciones, es decir, un mecanismo se evalúa por la capacidad de detección de los ataques, por el impacto

producido por los mismos, por el tiempo de resolución de dicho impacto y por el tipo de actuación llevada a cabo para resolver el ataque. El mejor mecanismo es el que detecta todos los ataques que se producen, que proporciona solamente verdaderos positivos (no genera ni falsos positivos ni falsos negativos), y que no provoca impacto porque él mismo lo ataja.

La sobrecarga introducida por un mecanismo cuando actúa se mide de forma indirecta, por el tráfico que genera (incluyendo un contador de tráfico en los sensores, tramas enviadas y recibidas), por los retrasos (por el tiempo entre tramas recibidas con origen el nodo que se quiere medir), por el consumo excesivo de recursos (diferencia entre el consumo habitual de energía y el consumo cuando actúa).

3.5.3. Sistema de alarmas

El control de las alarmas se realiza en el NOC, el sistema experto realiza la evaluación del rendimiento, recopilando la información de las plataformas a las que se conecta. El estado de alarma de un servicio en un momento determinado es: “Todo parece correcto” (*All Seem Well ASW)*, cuando no hay condición de alarma. Cuando existen alarmas, éstas se pueden categorizar por su importancia como "*Minor alarm*", "*Major alarm*" o "*Critical alarm*". Al desaparecer la condición de alarma, ésta desaparece, y se genera un “cese de alarmas” "*Alarm Ceasing*".

A continuación se proporcionan los criterios de la gestión de alarmas:

- Cuando en la WSN se detecta un ataque, lo reporta a su EB. La EB tiene control de todas las acciones que se llevan a cabo para mitigarlo. Esta información se envía al NOC bien para informar del diagnóstico, de las acciones realizadas, o bien de las actuaciones que se deben realizar. A cada unos de estos mensajes hacia el sistema experto, se les asigna una categoría de alarma y un impacto.

- También se establece una política de escalado de la severidad de las alarmas por la acumulación las mismas, y otra política de decrecimiento de la severidad en caso de que no haya repetición de la alarma en un cierto intervalo de tiempo.

- Todos los datos de las alarmas, su actividad, inicios y ceses de alarma se almacenan en el alarmlog. En base a la información contenida en el alarmlog, se establecen las estadísticas de alarmas.

- El hecho de concentrar toda la información de alarmas ofrece la posibilidad de generar otras alarmas de mayor nivel, así como alarmas proactivas. Cada ataque a un servicio, se asocia con los mecanismos adecuados y al impacto que provoca, se anota "el tiempo hasta el cese de la alarma", "el mecanismo asociado" y el "código de finalización de la actuación".

Los mecanismos se evalúan en base a sus características y propiedades como las siguientes:

- Flexibilidad: Grado simplicidad (o complejidad) para cambiar o reajustar los mecanismos de seguridad.

- Capacidad de ser monitorizado o de avisar de que un ataque se está produciendo: este parámetro mide la capacidad del mecanismo de seguridad, de permitir ser monitorizado (si ésta capacidad no la proporciona el fabricante, debería ser desarrollada por los expertos humanos en TSES).

- Se hace también un control de cobertura de conocimiento disponible en BES, LES y TSES.

Toda esta información se analiza y se trata como plan de mejora continua del sistema. Cada alarma se contabiliza desde varias perspectivas, categorías, tipos de ataque, y se valora el servicio afectado (con el mayor detalle posible para el caso de responder a posibles penalizaciones) para cada origen de ataque, y servicio atacado. La agregación de datos se realiza de forma que se pueda analizar el grado de cumplimiento de los objetivos de seguridad y privacidad para cada tipo de usuario.

Ejemplo, métrica 1: Percentil 90 de que las incidencias de categoría 2 tenga un tiempo de resolución, menor que el especificado para el servicio. Se almacena el tiempo de resolución de cada incidencia, se organiza en percentiles y se compara el percentil 90 con el tiempo objetivo especificado. Se reportan por separado las incidencias fuera de objetivos.

Ejemplo, métrica 2: Es el Indicador de disponibilidad (sin incidencias)

$$Coef(Sin\ ataques) = \frac{\mathrm{MTBF(v+,f-)}}{\mathrm{MTBF(v+,f-)+MTTR(v+,f-,f+)}}\ ; \qquad (1)$$

Donde MTBF es el tempo medio entre fallos (ataques), *(Mean time Between failures*) y MTTR es el tiempo medio de reparación (*Mean time to repair*).

Cada ataque, provoca unas consecuencias con un determinado alcance, sobre alguno o a varios de los servicios de seguridad definidos, afectando a los activos que deberían permanecer protegidos, este es el "Servicio de seguridad afectado". La "Severidad del impacto" representa la magnitud de la desprotección de los activos y sus consecuencias, éstas se caracterizan por la severidad, desde 0 (la más baja) hasta 3 (la más alta).

Los ataques se evaluarán teniendo en cuenta tanto los servicios de seguridad afectados, como la severidad del impacto. Cada ataque que se detecta produce un evento, estos eventos pueden ser categorizados como alarmas según el impacto producido. Si al realizar el análisis (ya sea manual o automático) se considera que hay alarmas y eventos relacionados con un origen común, la relación entre todas estas alarmas y eventos se establece asociándolos a un "evento raíz", con la finalidad de tener una visión completa de todo el entorno relacionado y poder ajustar el sistema para disminuir el número de Falsos Positivos y de Falsos Negativos, efectuando así un proceso de mejora continua y de automatización de soluciones a problemas ya conocidos.

Así, un "evento raíz" (ER), es un problema que puede tener relacionado varios eventos sin alarma, varios eventos con alarma, y quizá varias alarmas detectadas a posteriori (falsos negativos) que tras un análisis, se detecta que ha tenido como origen el mismo problema raíz. ER = {Ev1,….Evn} representa un conjunto de eventos relacionados que pueden tener o no, cierta categoría de alarma, a la vez que cada evento puede haber sido detectado en el momento o bien a posteriori. En cualquier caso el conjunto ER representa "el entorno del problema". Este tratamiento posibilita el aprendizaje, y el aumento de la fiabilidad de las actuaciones preventivas, correctivas y proactivas permitiendo así, unificar las mejores soluciones para cada caso y predecir efectos ante una misma causa conocida. Quizá si aparecen alarmas y eventos enraizados, la solución definitiva no sea resolver cada una individualmente, sino resolver la causa común.

```
ERx = {
      [Ev1; Detección; Impacto; Magnitud; Categoría; Causa]
      [Ev2; Detección; Impacto; Magnitud; Categoría; Causa]
      .
      .
      [Evk; Detección; Impacto; Magnitud; Categoría; Causa]
      }
```

Por lo tanto, para todo evento raíz (ER_x), existe una $Solución_x$, tal que dicha $Solución_x$ soluciona todos los eventos individuales que componen el evento raíz Ev_i; donde i є [1, k]. Si alguno de los eventos que componen el evento raíz Ev_i no se soluciona con la $Solución_x$ es un testigo de que, bien la solución aplicada no es completa, bien que el evento Ev_i no forma parte del problema raíz ER_x. o que también es parte de otro problema.

Cuando aparece un nuevo problema, se buscan antecedentes ya resueltos, y si los encuentra accede al espacio de soluciones, las aplica (si son aplicables), o bien las reporta junto con el evento raíz, o con el evento individual si no pertenece a ningún elemento raíz. En la figura 8 se esquematiza el sistema de evaluación del rendimiento.

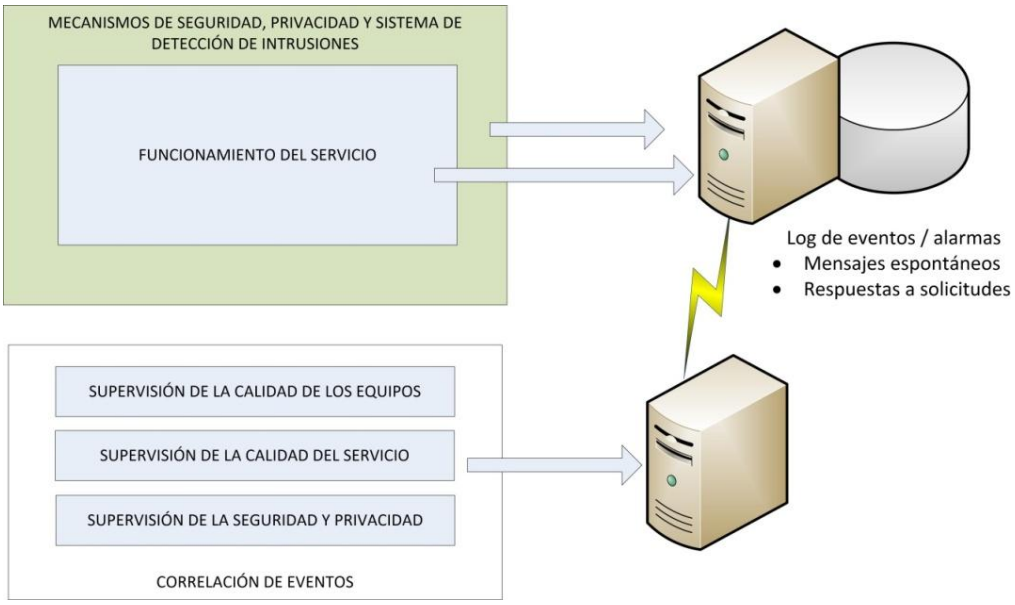


Figura 8. Sistema de evaluación del rendimiento.

3.5.4. Ahorro de costes

La posibilidad de especificar los servicios de seguridad a medida (no solo de la aplicación, sino del usuario final), en lugar de proporcionar todos por defecto, introduce un ahorro de costes.

Como se ha visto, la necesidad de privacidad de un servicio de IoT depende del marco legal al que esté sometido, marco que a su vez depende, tanto del propio servicio como de la utilidad que proporciona al usuario. Se ha visto también que el tipo de usuario monitorizado por el servicio (objetos, animales, personas) es fundamental para conocer el marco legal que se debe aplicar, para obtener así el nivel de protección necesario.

Supóngase que un determinado servicio va a ser aplicado a un conjunto de usuarios, a los que se clasifica en “n” ***Tipos de usuarios***, denotados Usu (i), donde i=1...n. Así, se podría formar un vector de los n ***Tipos de usuarios*** para representar la distribución de dichos usuarios en cada tipología definida: $\begin{pmatrix} A1\%\ Usu(1) \\ A2\%\ Usu(2) \\ . \\ An\%\ Usu(n) \end{pmatrix}$ (2) donde los valores *A*i representan los porcentajes de usuarios de cada tipo *Usu (i)*, con la condición de que $\sum_{i=1}^{n} Ai = 100$; es decir que el 100% de los usuarios del servicio caiga en alguno de estos tipos de usuarios definidos.

Sea la X, la matriz de asignación de servicios de seguridad, donde cada fila son los tipos de usuarios y las columnas habilitan o no los servicios de seguridad “1” habilitado y “0” deshabilitado. X = $\begin{pmatrix} b11 & . & b1k. \\ . & . & . \\ . & . & . \\ bn1 & . & bnk. \end{pmatrix}$ (3)

donde sus elementos son denotados por b[i,j] donde i=1...n y j=1...k es el valor que habilita o deshabilita el servicio “j” para el usuario “i” (las columnas representan “servicios de seguridad”, y las filas representan “Tipos de usuarios”).

El vector Y contiene los servicios de seguridad que el servicio final es capaz de proporcionar con la tecnología que se utiliza. Sus elementos son denotados como *ServicioSeg (j)* donde j=1...k. Y = $\begin{pmatrix} ServicioSeg(1) \\ . \\ ServicioSeg(k) \end{pmatrix}$ (4)

Por último sea el vector Z = $\begin{pmatrix} Servicios\ Seg\ Usu(1) \\ . \\ . \\ Servicios\ Seg\ Usu(n) \end{pmatrix}$ (5)

cuyos elementos representan el conjunto de servicios que deben asignarse para cada tipo de usuario, *ServiciosSegUsu (i)* donde i=1...n.

Así, mediante la operación:

X.Y =Z; $\begin{pmatrix} b11 & . & b1k. \\ . & . & . \\ . & . & . \\ bn1 & . & bnk. \end{pmatrix} . \begin{pmatrix} ServicioSeg(1) \\ . \\ . \\ ServicioSeg(k) \end{pmatrix} = \begin{pmatrix} Servicios\ Seg\ Usu(1) \\ . \\ . \\ Servicios\ Seg\ Usu(n) \end{pmatrix}$ (6)

se obtiene el conjunto de servicios que se debe aplicar a cada usuario, como resultado de operar las necesidades de protección (matriz X) con el vector de posibilidades tecnológicas (vector Y). Identificando el vector Z con el vector (2), se pueden obtener los ahorros de costes. Estos mismos cálculos se podrían orientar bien a servicios de seguridad (como se ha descrito) o bien a mecanismos de seguridad, para el caso de que haya mecanismos que comparten servicios o servicios que comparten mecanismos.

En el siguiente capítulo se expondrán algunos ejemplos prácticos, y al final del apartado 4.2.6 se hace una valoración cuantitativa del coste en recursos de varios servicios de seguridad para un caso concreto. En base a estas valoraciones, se realizarán cálculos para visualizar el ahorro de costes descrito en este apartado.

Aunque se describirá con más detalle, se dará una breve descripción del ejemplo. Supóngase que se crea un servicio de vigilancia de salud, para 4 "***Tipos de usuario***", el tipo usuario Usu (1) son las vacas lecheras en una granja; el tipo de usuarios Usu (2) son caballos de carreras; el tipo de usuarios Usu (3) son futbolistas de un equipo de fútbol; y el tipo de usuarios Usu (4) son bomberos realizando una actuación de rescate. Como se verá en el capítulo siguiente cada tipo de usuarios, tiene unos requisitos de seguridad y privacidad diferentes, éstos requisitos se representan en la matriz X, y los servicios de seguridad que el servicio es capaz de proporcionar, se relacionan en el vector Y, aplicando la ecuación (6) se obtiene como resultado en vector Z en (7)

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} Autenticidad \\ Privacidad \\ Integridad \\ \text{Disponibilidad} \end{pmatrix} = \begin{pmatrix} 0\ (Sin\ Seguridad) \\ Aut + Priv \\ Aut + Priv + Int \\ Aut + Priv + Int + Dispo \end{pmatrix}; \qquad (7)$$

Así al tipo de usuario 1 le corresponde el valor 0, que indica que para este tipo de usuario no es necesario ningún servicio de seguridad ni privacidad. De la misma forma cada tipo de usuario, tiene un conjunto necesario de servicios de seguridad y privacidad, y cada uno de estos servicios, tiene un coste en recursos. Estos recursos empleados pueden medirse en la perspectiva que se necesite, ya sea en mili Amperios, si estamos evaluando consumo, en mili segundos si lo que interesa es el coste en retardo, o en euros, si lo que importa es el coste monetario.

Según se expondrá en el apartado 4.2.6, los servicios de seguridad contribuyen con los siguientes consumos extras: El servicio de Integridad contribuye con consumo

extra de 4.3 mA, la Autenticación con 3.1 mA, y la privacidad con 2.5 mA, y el servicio de disponibilidad no contribuye con un consumo fijo.

Se denominará RE al recurso de energía empleado con la finalidad de evaluar los consumos extra para los diferentes tipos de usuarios**:**

- Para los usuarios del tipo 1: Sin seguridad, no tienen gasto extra, $\mathbf{RE_1}$ = **0 mA**
- Para los usuarios del tipo 2: Aut + Priv, $\mathbf{RE_2}$ = 3,1 mA + 2,5 mA = **5,6 mA** extras;
- Para los usuarios del tipo 3: Aut + Priv+ Int, $\mathbf{RE_3}$ = 3,1 mA + 2,5 mA + 4,2 mA=**9,8 mA**;
- Para los usuarios del tipo 4: Aut + Priv+ Int+ Dispo, $\mathbf{RE_4}$ = 3,1 mA + 2,5 mA + 4,2 mA + Dispo = **9,8 mA + consumo extra del servicio de Disponibilidad" mA**

Se ha Llamado **RE** a los **Recursos empleados**; y llamaremos **RA** a los **Recursos ahorrados.** Conociendo la cantidad de usuarios y su distribución A1% para vacas lecheras, A2% para caballos de carreras, A3% para futbolistas y A4% para bomberos, se podrá calcular los recursos ahorrados. Este ahorro no solo se materializaría en consumo sino en capacidad de proceso, en retardos,... operando de manera similar. La conclusión es ahorrar en el dimensionado del servicio final para cada tipo de usuario, ajustando el tipo de nodos que se utilizarán, utilizando redes homogéneas o heterogéneas de sensores, etc.

3.6. Conclusiones

En el ambiente colaborativo descrito es posible ofrecer a los usuarios la confianza necesaria sobre la seguridad y la protección de sus datos personales. En IoT, la limitación de los recursos en las redes inalámbricas de sensores hace necesario el establecimiento de una seguridad a medida que evite poner en riesgo la calidad del servicio por agotamiento de recursos. En general donde coexistan varios servicios y varias tecnologías, la inteligencia y la toma de decisiones sobre las políticas de seguridad pueden integrarse en centros de operaciones de red debidamente certificados y reconocidos. Esto proporciona gran capacidad de gestión y control de cambios para mantener y actualizar remotamente la seguridad a medida para los productos y servicios de Internet de las Cosas.

Esta colaboración posibilitaría la emisión de certificaciones de confianza para las partes interesadas y eliminar las posibles barreras de desconfianza. Este entorno colaborativo ofrece las siguientes ventajas:

- las empresas dedicadas al diseño de nuevos productos y servicios pueden realizar simulaciones virtuales previas a la toma de decisiones sobre el mercado real;

- en el ámbito legislativo podrían evaluar el impacto en la sociedad y en el mercado, de las posibles modificaciones y nuevas legislaciones en esta materia pudiendo conocer, cómo y en qué medida afectarían a los productos y servicios existentes y sus futuras evoluciones;

- las áreas tecnológicas podrían conocer rápidamente los aspectos críticos que necesitasen nuevas investigaciones e innovaciones.

4 Validación del sistema

4.1. Entorno de validación del sistema.

La validación del sistema se ha realizado aplicando el método, a los siguientes casos de uso:

- Servicios llevables (wearable) con la plataforma AWARE[4].
- Servicios para red eléctrica inteligente (*Smart Grid*) sobre la plataforma ACCUS[5] de ciudad inteligente (*Smart City*).

A continuación se enumeran los componentes básicos que forman los entornos de validación utilizados:

- El sistema experto (decide las políticas de privacidad que han de implementarse).
- Las plataformas de servicios (reciben las políticas desde el sistema experto y gestionan las actuaciones necesarias para configurar las redes de sensores que soportan los servicios).
- Las redes de sensores que soportan los servicios.

En los siguientes apartados se mostrarán los resultados obtenidos al aplicar el método a diferentes casos de uso.

4.2. Servicios llevables

El primer escenario de validación se ha realizado sobre la plataforma AWARE, diseñada para proporcionar servicios de IoT sobre dispositivos llevables.

Esta experimentación ha servido para demostrar cómo para un mismo servicio de IoT (idéntico), y realizando exactamente las mismas medidas pero aplicadas a diferentes usuarios sometidos a monitorización, genera diferentes marcos de protección de datos personales.

La maqueta de diseño y pruebas (figura 9) se compone de una WSN, de una plataforma middleware orientada a servicios, Proyecto AWARE expuesto en Santos-

[4] AWARE (Accessible wearable device platform for smart environments) Proyecto parcialmente financiado por el Ministerio de Economía y Competitividad ref.: TEC2011-28397.

[5] ACCUS (Adaptive Cooperative Control in Urban Systems) proyecto parcialmente financiado por el Ministerio de Industria, Energía y Turismo Ref. ART-010000-2013-2 y por Artemis JU (GA number 333020-1).

Familiar et al [154], y del sistema experto PDPS-IOT (*Personal Data Protection System for Internet of Things*) en Sánchez-Alcón et al. [2].

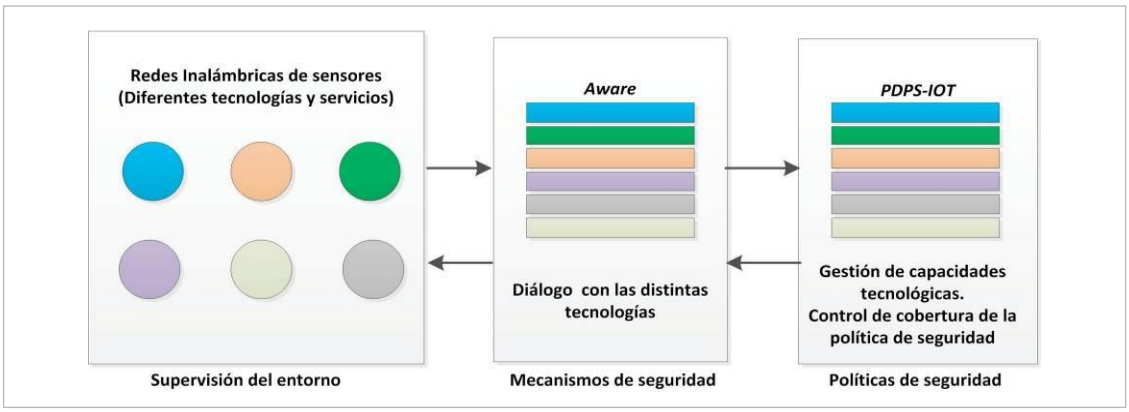


Figura 9. Maqueta de diseño y pruebas.

El sistema experto PDPS-IOT tiene como misión decidir la política que se ha de aplicar al servicio. Esta política se comunica a la plataforma AWARE (Accessible wearable device platform for smart environments), quien conoce bien a las WSN que gestiona (su tecnología, la forma en que debe dialogar con ellas, sus posibilidades, los mecanismos de seguridad que soportan, etc.) y es capaz de manejar sus posibilidades de configuración y generar los comandos y acciones adecuadas para configurarlas remotamente. PDPS-IOT conoce el conjunto de posibilidades que las plataformas (en este caso AWARE) es capaz de gestionar, de esta manera se puede establecer un nivel de seguridad homogéneo y coherente para todas las redes WSN, es decir proveer niveles equivalentes de seguridad, ya que las distintas tecnologías tienen sus propias particularidades y limitaciones. Aunque quien conoce bien a las redes de sensores son las plataformas, PDPS-IOT debe conocer las posibilidades de cada una de ellas para evitar pedir lo imposible.

El servicio final que se utiliza para esta prueba conceptual es la monitorización de la salud, recopilando datos de pulso y temperatura corporal. Estos datos se procesan y se envían a la estación base para informar a un equipo médico. Este servicio de monitorización de la salud se aplicará a los casos de uso planteados en Sánchez-Alcón et al. [2], donde se usa exactamente el mismo equipamiento técnico para proporcionar el mismo servicio final (un cinturón pectoral con sensores para vigilar, registrar y generar alertas sobre el estado de salud), pero utilizados para diferentes usuarios:

- Para monitorizar la salud de las vacas lecheras de una granja;
- Para monitorizar la salud y rendimiento de caballos de carreras;
- Para monitorizar la salud y rendimiento de un equipo de fútbol;
- Para monitorizar el estado de salud de un equipo de bomberos y de las víctimas en sus actuaciones.

Se aplica el RD 1720/2007 de protección de datos personales, y el borrador del Reglamento general de protección de datos de la Unión Europea. En los siguientes subapartados se describen los aspectos fundamentales del razonamiento.

4.2.1. Caso 1. Granja lechera

Es un servicio de ámbito privado cuyo objetivo es controlar la salud del ganado. No involucra datos personales. La información recopilada no es útil para nadie, excepto para el ganadero. No es un servicio crítico (estas mediciones no suplen a los controles alimentarios) y no tiene requisitos especiales de continuidad del servicio. El acceso al sistema se hace por usuario y contraseña sin mecanismo adicional, no implica una autenticación especial.

Comentarios: Muy distinto hubiera sido el marco asociado a un servicio donde una Central lechera, utilizara el mismo servicio para monitorizar a las vacas del conjunto de granjas que le suministran leche. Aunque las medidas no suplirían los controles sanitarios, pudiera haber fraude en cuanto a que alguna granja quisiera ocultar o falsear datos de sus vacas a la Central lechera, en este caso habría que añadir el marco de relaciones comerciales establecido entre las partes.

4.2.2. Caso 2. Caballos de carreras

Es un servicio de ámbito privado cuyo objetivo es controlar la salud y el rendimiento sus caballos. No involucra datos personales. El impacto de un posible espionaje de resultados podría ocasionar fraude en apuestas por lo que se protege el servicio contra: revelación/divulgación, veracidad de los actores y autorización del acceso. No es un servicio crítico, y no tiene requisitos especiales de continuidad.

4.2.3. Caso 3. Equipo de fútbol

Servicio de ámbito privado cuyo objetivo es controlar la salud de los jugadores. Hay datos personales que se deben proteger (como el estado de salud) por ley ante

revelación/divulgación por lo que se deben ocultar estos datos, o bien separar la identidad de la persona de sus medidas). Estos datos deben ser gestionados y manejados sólo por personal autorizado (veracidad de los actores y autorización del acceso). Se exige veracidad de los contenidos, según la ley los datos personales deben ser veraces (suponemos que los sensores están calibrados correctamente). Es un servicio que no es crítico y sin requisitos especiales de continuidad.

4.2.4. Caso 4. Equipo de bomberos

Servicio que debe ser homologado para controlar la salud de los bomberos y posibles víctimas. Hay datos personales que se deben proteger (por ejemplo el estado de salud) por ley ante revelación/divulgación se deben ocultar estos datos o separar la identidad de la persona de sus medidas. Estos datos deben ser gestionados y manejados sólo por personal autorizado (veracidad de los actores y autorización del acceso). Se exige veracidad de los contenidos, según la ley los datos personales deben ser veraces (suponemos que los sensores están calibrados). El servicio es crítico y necesita “continuidad del servicio” (llevan sensores en su equipamiento para que los médicos controlen el estado de salud de los bomberos y de los posibles rescatados). En caso de desconexión de la red, los sensores deben poder seguir siendo operativos funcionando en modo autónomo y generando alarmas audibles–visibles ante problemas de salud.

4.2.5. Resultados generales

La cobertura de privacidad puede cumplirse para los cuatro casos, porque el tipo de red considerado (la WSN) soporta los mecanismos que se necesitan y la plataforma AWARE los puede configurar. Los imperativos obtenidos de LES, se mapean en servicios de seguridad para poder compaginar los conceptos con el lenguaje técnico de seguridad. La Base de conocimientos tecnológicos, establece una relación conceptual directa entre los imperativos legales obtenidos de LES y los servicios de seguridad de la Recomendación X.800 [18] en TSES (tabla 10).

Imperativos de seguridad	Servicios de seguridad
Veracidad de los actores	Autenticidad
Autorización de acceso	Control de acceso
Divulgación o difusión de la información	Privacidad
Veracidad del contenido	Integridad
Responsabilidad Actores	No repudio
Disponibilidad y continuidad del servicio	Disponibilidad

Tabla. 10. Relación de imperativos de seguridad - servicios de seguridad.

Teniendo en cuenta el mapeo de resultados obtenidos por LES se obtiene la tabla 11 que esquematiza los resultados:

	Autenticidad	Privacidad	Integridad	Disponibilidad
Granja	-	-	-	-
Caballos	X	X	-	-
Equipo futbol	X	X	X	-
Bomberos	X	X	X	X

Tabla. 11. Valores típico en función del tipo de dispositivo.

Los ataques contra el servicio final, se afrontan mediante un conjunto de servicios de seguridad, que se concretan en contramedidas o mecanismos de seguridad que la base de conocimientos en TSES relaciona con dichos ataques. Este ejemplo se ajusta a los mecanismos disponibles en la WSN de pruebas que se muestra en la tabla 12, que corresponde con la propuesta “SensoTrust” de Castillejo et al. [155] para la plataforma AWARE.

Ataque	Ataque contra	Impacto	Mecanismo / Contramedida
Denegación de servicio (DoS)	Disponibilidad	Impide la comunicación: -Por interferencias. -Un nodo malicioso envía paquetes para confundir a la red. Desconexión de la red.	**Alarma DoS** En ambas situaciones, se activa una “alarma DoS” para alertar al personal de seguridad de la situación. Nodo da alarmas audible y lumínica
Ataque Sybil	Autenticidad	Invalida la información de los nodos legítimos y modifica el enrutamiento. Se produce cuando un nodo malicioso presenta numerosas ID (identidades) a la red.	**ID de nodo, revocación de nodo** El nodo reinicia el mecanismo de confianza. Sólo el gestor de seguridad de la WSN tiene la lista completa de las ID. Puede revocar o apartar el nodo.
Corrupción de los mensajes	Integridad	El mensaje que llega al receptor es diferente del enviado por la fuente. Interceptado / modificado.	**Hash** Funcionalidad de cifrado para realizar un hash del mensaje.
Eavesdropping (escucha)	Privacidad	En la transmisión por radio, otros dispositivos pueden escuchar e interceptar la comunicación entre nodos.	**Keys (symmetric y PKI)** Se utilizan capacidades de cifrado simétrico y PKI.
Captura de nodos	Privacidad	Algún nodo es capturado y alguien accede a las claves secretas, ID de nodo, etc.	**Few crypto. Data stored** Minimizar en el nodo la información criptográfica y de seguridad que se almacena. Renovar las claves en la red.
Réplica de un nodo	Autenticidad, Control de acceso (CA)	Un ID es copiado en un nuevo nodo, se introduce en la red y es aceptado con el ID clonado como un nodo autorizado.	**ID de nodo, políticas de seguridad** 1. El ID del nodo, almacenaje externo en el gestor de seguridad, que controla los ID en la red. 2. Si el gestor de seguridad detecta dos nodos operando con el mismo ID, emite un protocolo de revocación del nodo y lo expulsa de la red.
Nodo falso	Autenticidad, Control de acceso, Integridad	Inyecta datos en la red para evitar la comunicación entre nodos legítimos mensajes falsos, peticiones continuas de autorización…	**ID de nodo, claves de dominio** Identificar el nodo falso y, mediante la renovación de la clave de dominio, descartar todos los mensajes enviados por él.

Tabla. 12. Relación entre mecanismos disponibles para las pruebas.

4.2.6. Desarrollo de caso. Equipo de bomberos

Supóngase que el promotor, un ayuntamiento de una gran ciudad, por ejemplo, quiere dotar a su servicio de bomberos de un equipamiento IoT para controlar su salud y la de las víctimas en las actuaciones. Se quiere que el servicio se componga de unos sensores embebidos en la vestimenta *"Wireless Body Area Network (WBAN)"*, para medir los parámetros que atestigüen el estado de salud.

Supongamos que en las actuaciones participan dos equipos de bomberos, el "equipo de rescate" y el "equipo de apoyo". En el "equipo de rescate" cada bombero lleva un nodo sensor en su ropa, y un conjunto de sensores para colocarlos sobre el cuerpo de las víctimas. Estos sensores tienen como finalidad que el equipo médico pueda monitorizar la salud tanto de los bomberos, como de las víctimas.

Los nodos sensores que se colocan sobre el cuerpo de las víctimas se conectan en estrella al nodo sensor del bombero que se lo coloca, el cual actúa como "cluster head". Los cluster heads (uno por bombero) se conectan al sink, formando una red totalmente conectada entre ellos. La misión del "equipo de apoyo" es recibir a las víctimas, identificarlas y llevarlas a un lugar seguro. Este "equipo de apoyo" también lleva sensores porque estos bomberos también pueden estar en peligro. Este caso ha sido publicado [156]

El servicio se apoya en la estructura de red que se quiere configurar como muestra la figura 10 (respetando el idioma original), en la que se puede apreciar que toda la información termina en la sede de los bomberos conectados a través del sink situado en el vehículo, a este sink se conectan tanto los bomberos del equipo de rescate (las víctimas a través de ellos) y el equipo de apoyo.

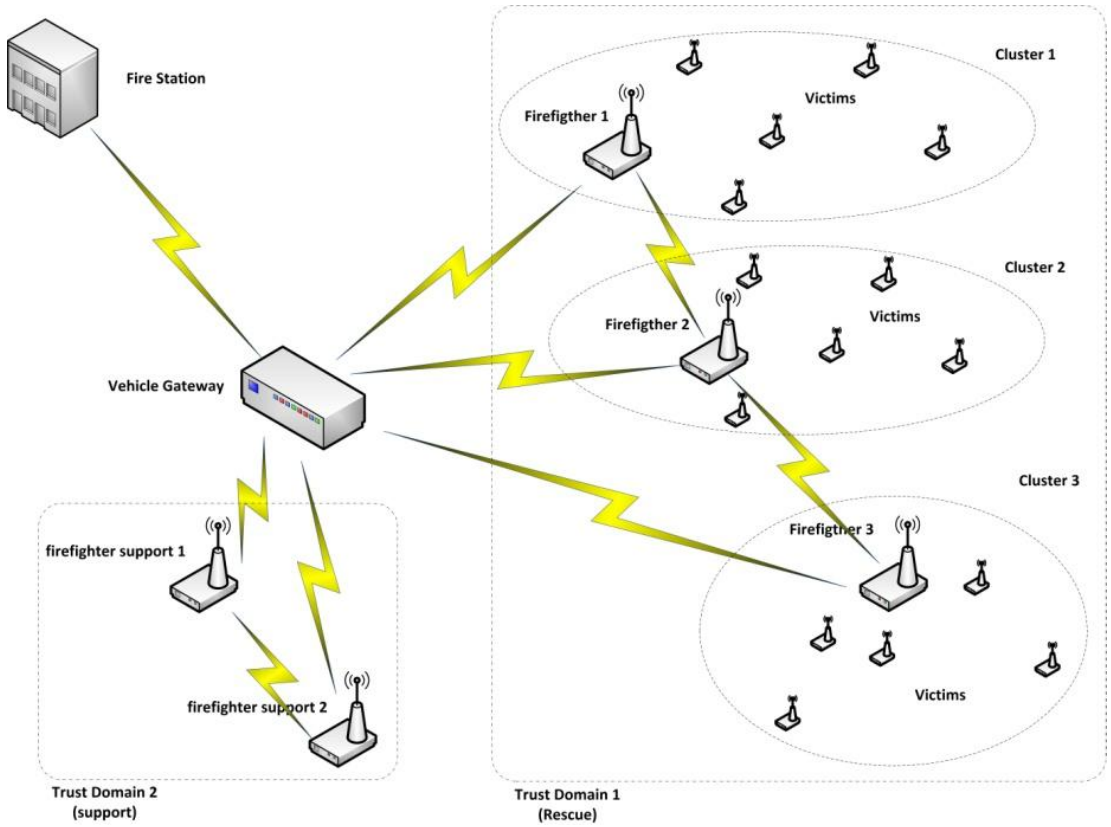


Figura 10. Esquema del servicio.

La primera etapa del proceso consiste en que BES confeccione la Matriz de Utilidad, en base a la información recopilada del promotor, mediante un conjunto de formularios guiados. Esta información se resume en la tabla 13:

MATRIZ DE UTILIDAD: Descripción del servicio		**Tipo de Red**	
Nombre del Servicio	Protección de bomberos y víctimas	Nombre de la Red	NW_Type1
Tipo de servicio	Health-care; Salvamento	Limitación de los recursos de los nodos sensores	Nodos Wearable: Capacidad de almacenamiento en memoria en modo autónomo
Tipo de entorno	Emergencias	Conectividad	Radio
País	España	Comunicación	
Promotor	Gobierno	Limitación en recursos de la EB	Ninguna
Usuario	Bomberos	Topología	Los Cluster heads totalmente conectados y la conexión entre víctimas y su cluster head, en estrella
Persona monitorizada	Bomberos y víctimas	Rol de los nodos	Recolectar parámetros de salud y del entorno
Capacidad legal de la persona	Varios	Enrutamiento	Jerárquico basado en cluster heads
Necesidades especiales	Varios		
Continuidad del servicio	Sí; (Debe operar en modo autónomo)		
Criticidad del Servicio	Alta		

Tabla. 13. Matriz de Utilidad: Del Servicio y del tipo de Red.

Supongamos que el servicio se utilizará en España donde 1- Los datos relacionados con el estado de salud de las personas se consideran datos personales que deben ser protegidos. 2- Los datos deben estar tan actualizados como sea posible, y verdaderos. 3- Los datos críticos para salvar la vida son prioritarios.

Los imperativos legales que deben actuar sobre la información sensible se muestra en la tabla 14 y las protecciones específicas sobre los datos se muestran en la tabla 15, ya en formato DPIA-T.

Este es un caso de dispositivos llevables (wearables) utilizamos el esquema propuesto en SensoTrust [155] que es un tipo de red conocido y con unos mecanismos ya desarrollados y conocidos. Se concentra toda la información en las siguientes tablas para mejor comprensión y economía de espacio, aunque se confeccionan en orden.

Sensor		Medidas	Tipo	Aut.	Integr	Priv	Dispo	Intruders insiders	Dominio de confianza
1	Bomberos	CO; humo; Gas	Vital para la vida	X	X	-	X	X	Dominio 1
2		Temperatura Pulso	Información privada	X	X	-	X	X	
3	Victimas	Temperatura Pulso Saturación de oxigeno		X	X	-	X	X	
4	Equipo de soporte a Bomberos y Victimas	Temperatura Pulso Saturación de oxigeno Identificación personal		X	X	X	-	X	Dominio 2

Tabla. 14. Conjuntos de datos y definición de los dominios de confianza.

DPIA-T : Solución de protección a Bomberos y Víctimas			
Servicio de seguridad	**Ataque**	**Objetivo**	**Defensa**
Disponibilidad	DoS	1- La capa física se degrada y la comunicación entre nodos es imposibilita (jamming). 2- Un nodo malicioso envía sus datos a la red.	Se debe detectar la situación para afrontarla
Autenticación	Sybil	Un nodo pide múltiples IDs, si el ataque tiene éxito puede destruir el mecanismo de confianza.	Restablecer la confianza expulsando al nodo malicioso.
	Nodo clonado	Cuando un node ID es copiado y replicado en un nuevo nodo que se introduce en la red	Detectar y revocar el nodo malicioso
	Nodo falso	Introduce tráfico en la red para evitar la comunicación de los nodos legítimos (Inyectando mensajes con datos falsos, reclamando continuamente autorización, etc.).	Identificar le nodo falso descartando todos sus mensajes.
Integridad	Mensaje corrupto	Un mensaje llega al receptor con un contenido diferente al enviado por la fuente.	Asegurarse de que los mensajes no han sido alterados.
Privacidad	Eavesdrop-ping (escucha)	Otros dispositivos escuchando en la misma frecuencia pueden interceptar las comunicaciones entre nodos.	Usar autenticación y cifrado. Anonimizar los datos.
	Captura de nodos	Un nodo es capturado y criptoanalizado (las claves secretas, ID de nodo, las políticas de seguridad, etc.	Pocos datos almacenados en los nodos y renovar las claves..

Tabla. 15. Imperativos legales en formato DPIA-T.

Se eligen mecanismos concretos que cumplan la política en cada dominio, utilizando los mecanismos técnicos de la figura 16 aportados por SensoTrust, que figuran en la base de conocimientos de TSES para el caso de este tipo de red y servicio.

		Política del Dominio 1	**Política del Dominio 2**
Servicio de seguridad	**Ataque**	**Contramedidas**	**-**
Avail.	DoS	Se dispara una alarma en el gestor de seguridad informando de la situación	**-**
Autent.	Sybil	Se preconfiguran las ID de los nodos, sólo el gestor de Seguridad tiene una lista completa de las identidades. En caso extremo se revoca el nodo.	
	Nodo clonado	El ID de nodo se almacena en una entidad externa que controla todos los ID en la red. Si el gestor de seguridad detecta que 2 nodos están operan con el mismo ID, se emite un protocolo revocación del nodo.	
	Nodo falso	Con el ID de nodo, el esquema es capaz de identificar el nodo falso y, se descartan todos los mensajes enviados por este nodo.	
Integ.	Mensaje corrupto	El esquema de seguridad incluye la suite de cifrado, que permite realizar un hash del mensaje.	
Priv.	Eavesdropping (escucha)	-	Proporcionar capacidades de cifrado simétrico y PKI. Anonimización (desvincular la id personal de sus datos)
	Captura de nodo	-	Minimizar la información criptográfica y de seguridad almacenada el nodo. Además todas las claves en la red se pueden renovar.

Tabla. 16. Asignación de mecanismos disponibles para las pruebas.

Según se muestra en la figura 11 (respetando el idioma original) se puede apreciar que los recursos en consumo energético, tienen un límite impuesto por el fabricante o bien por pruebas. En este caso se ha estresado un nodo sensor hasta el límite, en el caso de los nodos utilizados se ha puesto el límite Máximo en un 20% por debajo del umbral al que se alcanza el estrés. Hay que tener en cuenta que a veces este límite lo puede poner el propio servicio, pero este no es el caso.

A partir de aquí se ha probado con cada servicio de seguridad que se presta y el consumo que introduce en un nodo sensor, obteniéndose los valores de la figura 11. Se puede apreciar el consumo inicial en caso del nodo sensor en estado de reposo y sin tener equipado ningún tipo de seguridad. A partir de este valor se puede apreciar la contribución en consumo de los diferentes servicios de seguridad y privacidad.

El Gap considerado para no tener problemas de afectar a la calidad de servicio es un 20% del máximo, es decir un 40% por debajo de la medida de estrés

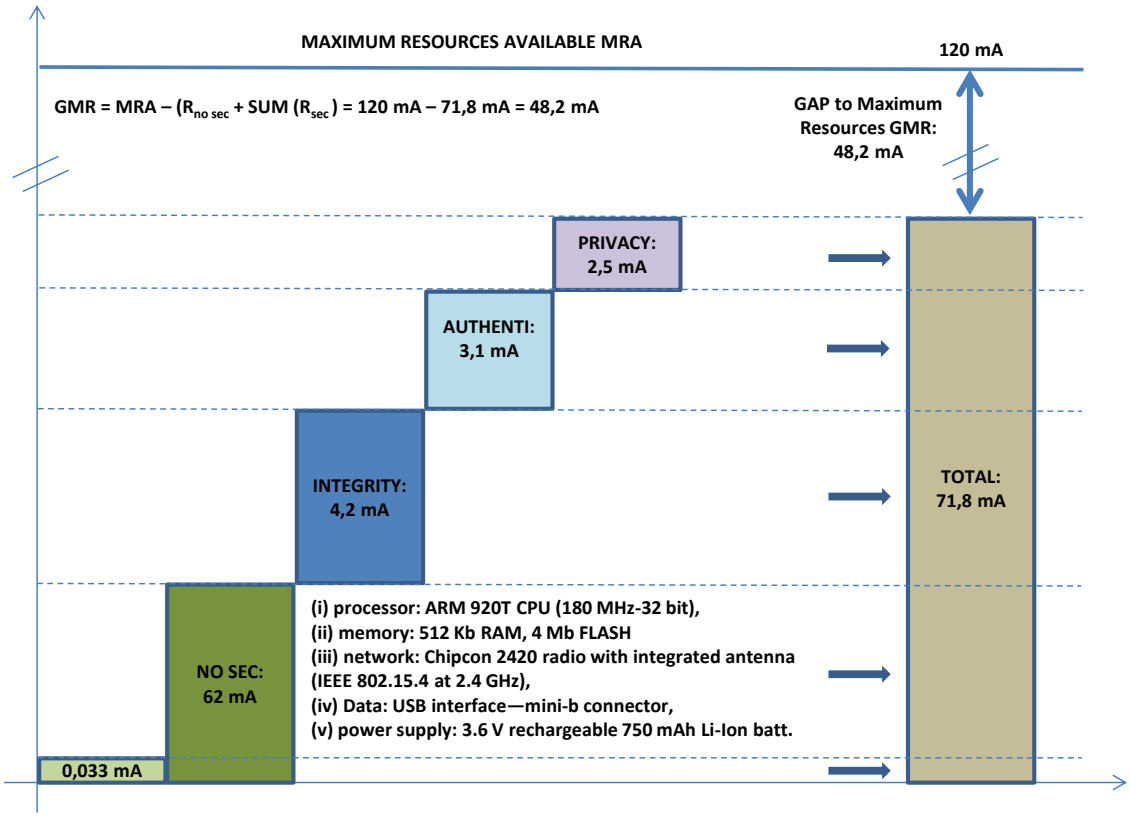


Figura 11. Gasto de recursos.

4.3. Servicios para red eléctrica inteligente

El servicio global prestado por una ciudad inteligente o Smart City, está formado por un conjunto de servicios individuales capaces de colaborar entre sí para dar unos servicios de mayor valor añadido. Estos servicios están controlados por unos sistemas urbanos. El control y la gestión de todos los elementos de red distribuidos por la ciudad pueden ser reconfigurados. Estas acciones, pueden llevarse a cabo forma automática, mediante la plataforma ACCUS que actúa como mediador, es decir, debe ser capaz de traducir la política de seguridad y privacidad, recibida del Sistema Experto, y generar los comandos y las acciones necesarias, adaptadas a los requisitos de las tecnologías de la ciudad inteligente, activando así los mecanismos adecuados.

Esta tarea de configuración y reconfiguración de la política de seguridad y privacidad de la Smart City se lleva a cabo mediante el uso de la cadena de mediación mostrada en la figura 12 (respetando el idioma original).

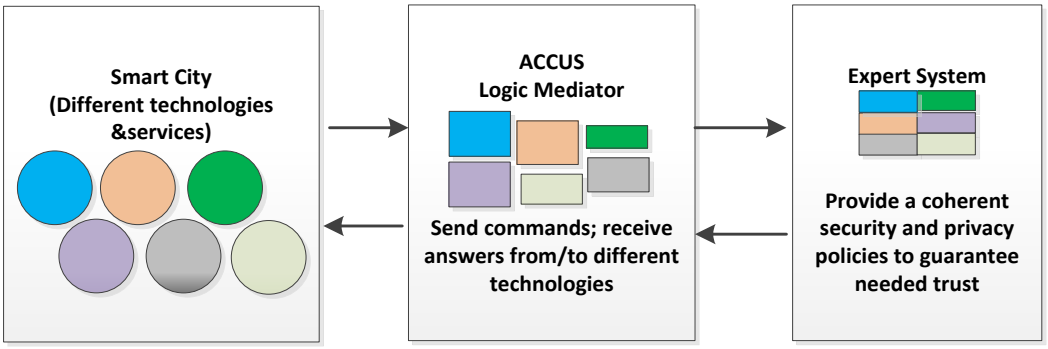


Figura 12. Cadena de mediación.

La Figura 13 (respetando el idioma original) muestra un esquema conjunto entre el entorno de colaboración que genera el conocimiento requerido e interactúa con el sistema experto, y la plataforma ACCUS, que comprende y mantiene un diálogo con los sistemas y elementos de la ciudad.

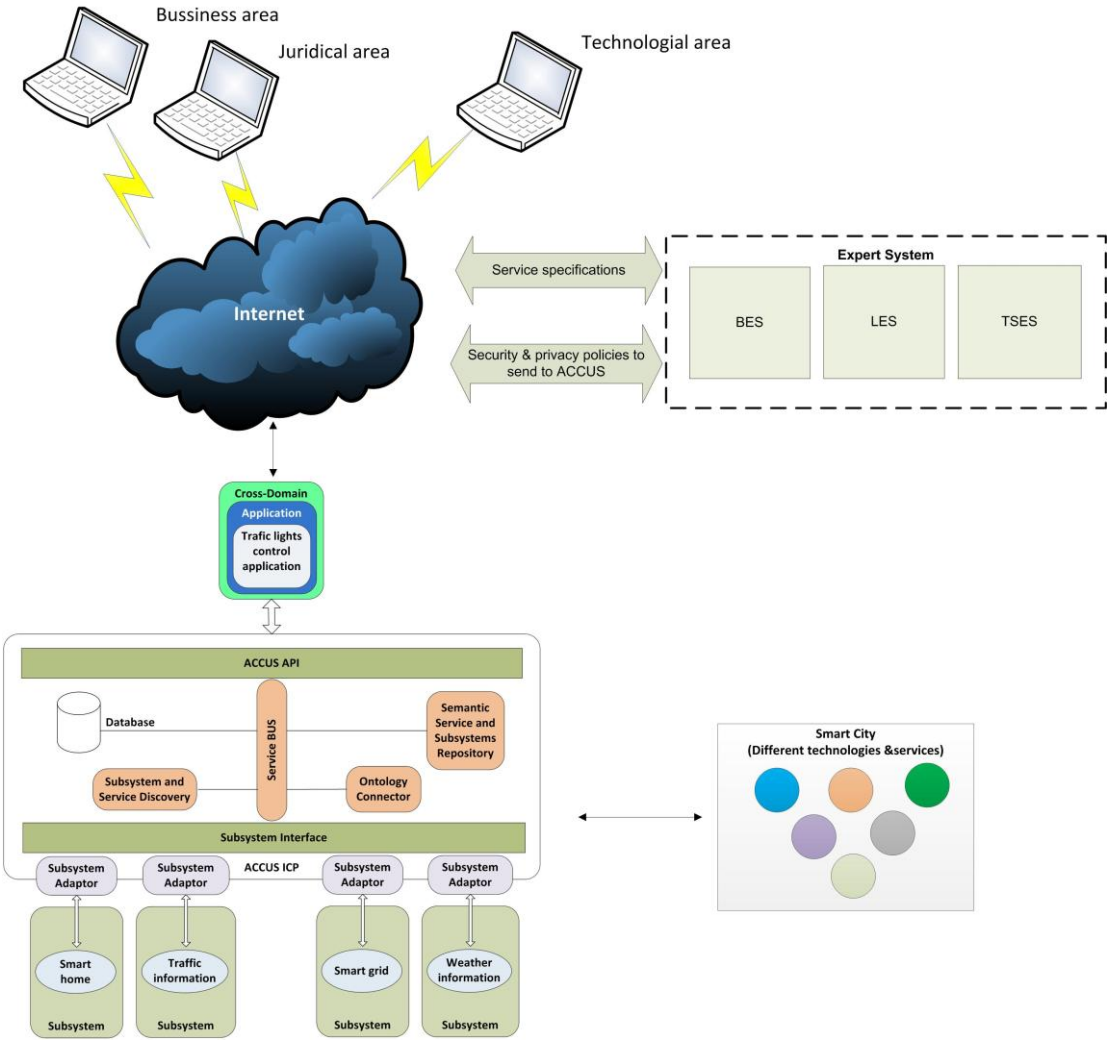


Figura 13. Visión general de la operación del sistema.

Las pruebas de validación se realizarán sobre el servicio de red eléctrica inteligente (*Smart Grid*). Este servicio se compone de dos tramos significativos de red, el tramo denominado del "hogar" donde se encuentran los contadores del consumo eléctrico o también llamado contador inteligente "*Home Meter*", y el otro tramo es la red de generación, transporte y distribución eléctrica.

En el caso de Smart Grid, la mayor parte de la información de la Matriz de Utilidad y de los datos personales implicados se omite, porque ya implícitamente se incluye en la DPIA-T que ya nos viene dada para este servicio. El análisis jurídico ya está realizado, por el "Grupo de Trabajo de la Smart Grid [150], en conformidad con la legislación en vigor.

Estas plantillas se componen de un conjunto de tablas donde reflejan las amenazas que pueden poner en peligro la confidencialidad, integridad, disponibilidad, etc. Estas tablas incluyen las amenazas genéricas que pueden conducir a situaciones no deseadas, tales como infracciones de procesos o el uso de los datos personales, la falta de disponibilidad de los procesos o procesamiento, desaparición de los datos personales. El contenido proporciona las amenazas genéricas a una Smart Grid; explicando las amenazas; dando unos ejemplos específicos en la industria de energía; así como el control genérico que debe aplicarse.

También ofrece información relativa a los “eventos temidos”, que identifica las amenazas; los objetivos relacionados de seguridad y privacidad, los activos afectados, el impacto; la probabilidad; y el Nivel de Riesgo, es decir, los imperativos de seguridad y privacidad necesarios en este servicio sobre los datos que se deben proteger.

4.3.1. Ataques y objetivos vs contramedidas

Cuando se establecen dominios de confianza para aumentar la seguridad y privacidad de las soluciones, se ha de realizar tanto la "definición de la confianza" como "los dominios de confianza”. Se deben desarrollar también todos los elementos involucrados (claves, roles, políticas). Se deben especificar también las acciones que deben realizarse cuando un dominio ya no sea de confianza, efectuando una validación de los dominios de confianza.

La política de seguridad para cada uno de los dominios de confianza se define para garantizar que la información confidencial será protegida. La tabla 17 se utiliza para establecer las políticas teniendo en cuenta los posibles ataques, con los servicios de seguridad necesarios para afrontarlos.

Para un entorno como el Smart Grid [157], se propone una solución para asegurar la red inteligente que incluye estándares de PKI, Smart Grid PKI tools, certificación de dispositivos, Trust Anchor Security y Certificate Attributes.

En [158] se propone cómo hacer una Smart Grid segura mediante la interconexión de dominios de confianza y define Trust anchors, que gestionan la distribución de claves dominio; cada trust anchor tiene una clave pública y una clave privada. Los Agregadores de datos, que son los agentes capaces de realizar tareas de procesamiento de datos complejos, también se definen (cada agregador de datos tiene una clave pública certificada y una clave privada para comunicaciones de datos).

Los recolectores de datos, son controlados por agentes de detección, así cada recolector de datos tiene una clave pública certificada y una clave privada para comunicarse con otros dominios. Los sensores tienen una tarjeta inteligente que contiene dos certificados para la delegación de confianza emitido por Trust anchors, estos certificados facilitan las comunicaciones seguras desde los sensores a otras entidades destacadas del dominio.

Para realizar este ejemplo, la información básica en la base de conocimientos de TSES se ha obtenido del artículo " *Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures*" [159], y otros artículos [160-181]. Con la información recopilada de estos artículos, se definen las tablas 17-23 relacionando los posibles ataques u objetivos, con los servicios de seguridad en el entorno de red inteligente y los mecanismos disponibles del siguiente apartado.

En las siguientes tablas se respetará el idioma original (inglés) para facilitar el seguimiento con la documentación antes referenciada aunque los comentarios se realizarán en el idioma de la tesis.

Security services: Authenticity (**Authe**); Authorization (**Autho**); Availability (**Av**); Confidentiality (**Conf**); Integrity (**Int**); Non repudiation (**NR**)

TARGET	***ATTACKS***	***Authe***	***Autho***	***Av***	***Conf***	***Int***	***NR***
Consumption reporting (devices)	Eavesdropping; Traffic Analysis; Message Modification; Replay; EMS Impersonation.	X			X	X	
Energy Services Interface/Home Area Networks	Repudiation; Message Modification; Replay	X				X	X
Meter tampering	Tampering/Reversal; Removal of Meter; Illegal Software Modification / Update	X				X	
Remote home monitoring and control	Customer Impersonation; Device Impersonation; Message Modification; Replay; Repudiation	X				X	X
Requests for data	Customer Impersonation; Eavesdropping; Message Interception; Message Modification	X			X	X	
Aiming the Demand	ESI Impersonation; Message	X		X		X	X

Security services: Authenticity (**Authe**); Authorization (**Autho**); Availability (**Av**); Confidentiality (**Conf**); Integrity (**Int**); Non repudiation (**NR**)							
TARGET	***ATTACKS***	***Authe***	***Autho***	***Av***	***Conf***	***Int***	***NR***
Response signals at the ESI/HAN	Modification; Replay; Jamming Attacks; Device Impersonation; Repudiation						
Outage Reporting	Meter Impersonation; Replay	X		X		X	
The Distributed Energy Resources (DER) shutdown/isolation reporting.	Meter Impersonation; Message Modification; Replay					X	
The Neighborhood Area Networks (NAN) aggregator	Eavesdropping; Message Meditation; Man in the middle; False Data Injection; Denial of Service.	X			X	X	
The Demand Response signals to the ESI/HAN	Message Modification; Impersonation of DRMS / LMS; Replay of Previous Messages; False Synchronization Attack.	X				X	
The Direct Load Shedding signals to the ESI/HAN.	Denial of Service; Access the DRMs/LMS server; false synchronization attack; Replay	X		X		X	X
The Energy Import/Export signals to the ESI/HAN.	Replay attack; Message Modification; Denial of Service	X		X		X	
The customer related data forwarded to a third trusted Energy Service Provider (ESP)	ESP Impersonation; Eavesdropping	X			X	X	
Steal data from utility servers.	Publicly available info; Weak platform config.; Software vulnerabilities; Malware Insider attacks	X	X	X	X	X	
Take control of utility servers.	Publicly available info; Weak platform config.; Software vulnerabilities; Malware; Passive Net Recon.; Message Fabrication; Replay; Fiddling with system / non system files	X	X	X	X	X	X
Take down utility servers.	Eavesdropping; Traffic Analysis; Man-In-The-Middle; Message Modification; Replay Attack; Device Impersonation; Denial of Service; Fiddling with system / non system files.	X	X	X	X	X	
Massive attack against equipment of measurement	False Data Injection; Malware			X		X	

Tabla. 17. Servicios de seguridad vs ataque para una Smart Grid.

Todos estos ataques pueden ser realizados tanto por outsiders como por insiders. Estos últimos sin embargo, pueden realizar actuaciones más perjudiciales. En los ataques internos se puede realizar un mal uso de los sistemas [182] que disponen de componentes de software importantes como los Interfaces Hombre Máquina (HMI), los servidores con los datos históricos en la estación principal, RTUs en subestaciones y enlaces de comunicación entre ellos. Los operadores usan los datos del HMI para tomar decisiones de supervisión sobre el control de las RTU. Por lo tanto, HMI, los datos históricos, RTUs, enlaces de comunicación, los valores umbrales y los ajustes normales de los sensores y actuadores [183] pueden ser atacados por outsiders (que generalmente son oportunistas, deliberados, y maliciosos) o por insiders (un usuario autorizado que hace mal uso de los permisos y daña el sistema mediante el envío de comandos de control legítimos con un gran impacto y mayor tasa de éxito. Estos ataques son difíciles de predecir y protegerse contra ellos). Hay dos grandes tipos de insiders, los ingenieros (responsables de la gestión de librerías de objetos e interfaces

de usuario, de la configuración de la topología de red, de los estados normales de condiciones de trabajo, el establecimiento de parámetros de dispositivos, la definición de los puntos de ajuste de procesos, escribir los scripts de automatización, etc.) y los operadores (que supervisan el estado del sistema en los servidores HMI, que reaccionan a alarmas y algunos eventos para que el proceso funcione correctamente, ejecutan comandos de operador que pueden impedir la activación de nuevas alarmas, también resuelven las alarmas entrantes, y toman decisiones sobre el cambio de topología , etc.). Cada uno con sus conocimientos y accesos tiene un poder de actuación y por tanto de atacar a distinto nivel. Los ataques internos [182] más usuales son:

- Las “Alarmas sin resolver”, cuando las alarmas se retrasan, se actúa incorrectamente o de forma incompleta. Estas situaciones pueden provocar fallos en cascada provocando mayores consecuencias. Podría también darse el caso de que esta disfunción en la resolución de las averías e incidencias pudiera ser consecuencia de decisiones empresariales sin una adecuada gestión del cambio, tales como recortes presupuestarios, implantar un plan de transformación de la actividad de los operadores ampliando por ejemplo, su ámbito de actuación desde una especialidad concreta a un cierto grado de multifuncionalidad, sin la formación adecuada o la experiencia suficiente, entre otros.

- “mala configuración”: pueden provocar sobrecargas cuando se realizan cambios incorrectos de las transferencias de topología y de carga, también pueden causar interrupciones mediante la apertura de los alimentadores de salida, y un funcionamiento incorrecto de los equipos causados por ajustes incorrectos. La demostración de que estas anomalías proceden de ataques, es complicada porque cualquier pequeño error, puede provocar la pérdida de piezas importantes que puedan evidenciar y hacer las pruebas inadmisibles para las acciones judiciales que requieran.

Algunos mecanismos contra los ataques internos [182], se enumeran a continuación:

- Detectar comportamientos anómalos en el tráfico de red, de una SCADA.
- Detectar anomalías basado en los protocolos de validación de las especificaciones

- Detectar las anomalías provocadas por los ataques internos mediante los registros del sistema, monitorizando periódicamente para detectar comportamientos anómalos.

- Incluir un módulo capaz de entender las acciones del usuario. El Statistical Anomaly Detection Method (SADM) se basa en el análisis de las propiedades estadísticas de las alarmas que determinarán el comportamiento normal del sistema. SADM determina si hay una desviación significativa entre "el comportamiento actual" y la "conducta normal" que aprende de las observaciones del comportamiento del operador.

- En Colored Petri Nets - CPN - modelo de los ataques internos [184] comenta que cualquier comportamiento malicioso que cambia las propiedades estadísticas de las alarmas y se identifica como una anomalía.

4.3.2. Servicios y mecanismos de seguridad

Una vez confeccionado el mapa de servicios de seguridad para proteger la Smart Grid visto en la tabla 17, el siguiente paso es buscar en la base de conocimientos de TSES, el conjunto de posibles mecanismos técnicos disponibles que puedan afrontar esos ataques. El conjunto de mecanismos para hacer frente a los ataques se representan en las tablas 18-23, cada una de estas tablas representa mecanismos que se pueden aplicar a los elementos de la red, con el fin de obtener los servicios de seguridad y privacidad necesarios de acuerdo a la política requerida.

Authenticity Mechanisms	***Description***
Keyed cryptographic hash functions	Similar to cryptographic hash functions, but making use of a secret key, are message authentication codes such as HMAC [185].
Physically Unclonable Functions	The use of Physically Unclonable Functions [160] modules within meters for achieving strong hardware based authentication of smart meters and efficient key management. PUFs are functions embodied in a physical structure inexpensive to manufacture but impossible to replicate even given the exact manufacturing process.
Hash based authentication codes	In [186] propose a lightweight message authentication outline as a crucial component of their envisioned framework. Their proposed outline based on Diffie-Helman key establishment and hash-based authentication codes.
MAC-attached and HORS-signed messages	Message Authentication Codes and One-Time Signatures were all evaluated for their ability to ensure message authenticity and integrity while not violating the stringent timing requirements introduced by certain message categories and despite being run on devices with limited processing power [187].

Tabla. 18. Mecanismos de Autenticidad.

Authorization Mechanisms	***Description***
Attribute Based	Access control proposed by [188]. An outline of this mechanism is introduced. Collected data are encrypted under a set of attributes before sending. These attributes

Authorization Mechanisms	***Description***
Encryption	could be any information related to that data like the source of energy, the user type, etc.
Attribute Certificates	In [189] give the idea of public key certificates and zero knowledge systems for the purposes of authentication and the idea of attribute certificates (ACs) for authorization.
Attribute Based Access Control System based on XACML	Jung et.al. in [190] various attributes associated with a user are given as input to the function that determines whether a user can access a particular resource in a particular way.

Tabla. 19. Mecanismos de Autorización.

Availability Mechanisms	***Description***
Against DoS attacks aiming to saturate the resources in order to prevent it from being accessible to its legitimate users.	
Alternate Frequency Channels according to hardcoded sequence	In [191] suggest an effective defense against jamming is to use multiple alternate frequency channels when interference is detected in the current channel. Nodes authenticated and introduced into the network receive this predefined channel-hopping sequence encrypted with the customer‘s public key. The node then retrieves the sequence by decrypting with the customer‘s private key and begins communicating in the current channel used.
Frequency Quorum Rendezvous	In [192] propose a random spread-spectrum-based wireless communication scheme that prevents eavesdropping and active attacks, while also ensuring protection against jamming. Their scheme is called Frequency Quorum Rendezvous and introduces the novelty of coordinating two random hopping sequences using a quorum system, a property that guarantees the sender and the receiver will rendezvous within a bounded time.
Against Denial of Service attacks aimed at higher layers than the physical layer the Intrusion Detection System (IDS) is commonly used. IDS can be classified into three categories [193]:	
Signature-based IDS	Recognizes intrusions using a blacklist of known attack patterns. Not adequate for Smart (Home/Grids)
Anomaly Based IDSs	Recognizes deviations from what is considered to be normal, by building a model of normal system behavior where any deviation from normal is identified as an intrusion. Adequate for Smart (Home/Grids)
Specification Based IDSs	Detects attacks using a set of constraints (rules) defining the correct operation of a program or protocol. Adequate for Smart Grids

Tabla. 20. Mecanismos de Disponibilidad.

Confidentiality Mechanisms [159]	***Description***
Symmetric/Asymmetric Encryption	Algorithms such as AES; RSA; ECC, etc.
Anonymization	Removes the link between data and its origin
Trusted Aggregators	Entities that can handle the aggregation of data can only use the aggregates of data without being able to have access to individual information.
Homomorphic Encryption	Allows computations to be carried out on ciphertext and obtain an encrypted result which when decrypted matches the result of operations performed on the plaintext..
Perturbation Models	Introducing random noise from a known distribution to the privacy sensitive data sources. When perturbed data are received, they are reconstructed in approximation to the original data. It must be a tradeoff between the level of privacy achieved and the information loss.
Verifiable Computation Models – Zero Knowledge Proof Systems	The aggregator provides a proof of the aggregate data sources.
Data obfuscation	Battery-based approaches that aim to conceal the amount of energy consumed.
This table is a subset of the Smart Grid Privacy preservation, a much more complete taxonomy is defined in [194].	

Tabla. 21. Mecanismos de Confidencialidad.

Integrity Mechanisms	***Description***
Cryptographic Hashing Techniques	The sending side uses a hash function to compute the checksum of the message to be sent and attach it to the original message [186]. The receiving side applies the same hash function to the message and compares the resulting hash to the hash attached in the original message. Should the two hashes match, integrity is verified.
Digital Watermarking	An efficient way to ensure defense against false data injection attacks. It is a technique that embeds digital data inside collected information to validate the integrity of data. This technique is used in high speed unsecured networks that are prone to false data injection attacks [195].
Adaptive Cumulative Sum Algorithm	A countermeasure against false data injection attacks [196] consisting of a recursive algorithm comprising of two interleaved stages. The first introduces the linear unknown parameter solver while the second applies the multi-threated CUSUM algorithm. The proposed defense mechanism aims at detecting attacks as quickly as possible with a minimum number of observations while maintaining a satisfactory level of accuracy.
Installation of known secure PMUs in network	The authors of [197] propose an algorithm for detecting stealth attacks and suggest the installation of known-secure phasor measurement units at specific buses, to thwart an arbitrary collection of attacks (not only sparse attacks).
Load Profiling	A countermeasure against device impersonation attacks [191]. When a device is advertised to the AMI, the AMI sends a previously formed load profile of that device to the outlet controlling the device so that a comparison can be made. If the loading pattern does not match the known profile then the outlet will not allow the device to operate.
Others	Sequence Numbers, Session Keys, numbers used once: counters against replay attacks. Many different countermeasures exist including the use of timestamps/sequence numbers/session keys [191], or including the use of numbers used once making each message unique [198].

Tabla. 22. Mecanismos de Integridad.

Non Repudiation Mechanisms	***Description***
Mutual Inspection with Smart Meters	Xiao, [198], show how the readings of the two ends are exchanged and the inconsistency is checked against an acceptable threshold. The authors compliment their approach with a security analysis and an evaluation that shows that satisfactory performance can be achieved when combined with an optimized time window method.
Unique keys for customer-AMI communication	Aravinthan, [191] suggest that both the customers and the AMI use unique keys for encryption (once they have authenticated one another using their preassigned public-private key pairs).
AMI transaction logging	AMI keeps a log of all transactions for a predefined number of days, so that disagreements can be resolved, though tracing back the events.

Tabla. 23. Mecanismos de No-Repudio.

Sobre la base de los mecanismos disponibles para la Smart Grid, el sistema tiene que seleccionar los mecanismos adecuados de entre ellos, para las partes de Home Meter, para la parte del agregador de NAM la Smart Grid, subestaciones, cabecera AMI, y las comunicaciones entre ellos, y equipos asociados.

Los criterios de selección de los mecanismos de seguridad por una parte, deben estar de acuerdo con el mapa de servicios de seguridad (tabla 17) y la extensión de los servicios (la parte del hogar, la parte de la red y la comunicación entre ellas).

Por otra parte, se debe tener en cuenta la eficacia de los mecanismos contra los ataques a la seguridad, y la sobrecarga puede causar en el sistema. Otro tema importante es la flexibilidad para cambiar o ajustar cada mecanismo, y, finalmente, es importante la capacidad para poder ser monitorizado. Lamentablemente esta información no siempre está disponible, puede que esa información sea ofrecida por el proveedor, de todos modos es posible proporcionar las experiencias pasadas sobre estos temas dentro del sistema, evaluando los resultados obtenidos.

En este caso, en la base de conocimientos de TSES no se dispone por el momento de datos antes mencionados, actualmente el sistema está en pruebas. Los resultados obtenidos con la estructura básica de la información, proporciona el siguiente conjunto de mecanismos:

- Physically Unclonable Functions (PUF) [160], Authentication, Confidentiality, Integrity
- Hash based authentication codes [186], Authentication
- MAC-attached and HORS-signed messages [187], Authentication, Integrity
- Attribute Based Encryption [188], Authentication, Authorization (HAN to BAN, BAN to NAN and NAN to RTU)
- Alternate Frequency Channels according to hardcoded sequence [191], Authentication, Authorization, Integrity. Replay attack
- Frequency Quorum Rendezvous [192], Availability, Integrity. Jamming
- Specification Based IDSs [193], Av. Eavesdropping, jamming. Physical attack
- Anonymization; Trusted Aggregators,[159] Authentication, Confidentiality
- Load Profiling [191], Integrity. against false data injection
- Sequence Numbers, Session Keys, numbers used once [192, 199], Integrity. Devices impersonation attack,

- Mutual Inspection with Smart Meters [198], Authentication, Non-Repudiation (inconsistencies detect attacks such as jamming)
- Unique keys for customer-AMI communication, AMI transaction logging [191], Authentication, Non-Repudiation
- Mecanismos relativos a las políticas generales de los equipos informáticos y base de datos, como Antivirus, Firewalls.

Cuanta más rica sea la información contenida en las bases de conocimientos, mejores resultados pueden obtenerse. Cuando se comunican estos mecanismos al ICP, tiene que tratarlo como otro servicio, es decir, como un servicio de seguridad para una Smart Grid. Este ICP debe aplicar mecanismos para que sean compatibles y resolver cualquier posible conflicto entre ellos.

5 Conclusiones y trabajos futuros

5.1. Mejoras proporcionadas por el sistema

La idea del modelo aportado por esta tesis sobre crear un ambiente colaborativo entre los promotores de los servicios, y los ámbitos jurídico y tecnológico para dar soluciones de seguridad y privacidad, ha sido difundida tanto por las publicaciones realizadas, como por la participación activa en foros de discusión sobre productos y servicios de IoT en las redes sociales. Esta idea ha generado una reacción positiva aunque bastante escéptica debido a la dificultad que representa impulsar este ámbito de colaboración, entre áreas que tradicionalmente han estado bastante separadas, y con formas de entender muy distintas. Esto implica que se han de abrir nuevas vías de participación y colaboración así como vencer las resistencias que inevitablemente puedan surgir. También es cierto que todos están de acuerdo en que contribuiría a eliminar en gran medida las lagunas legales generadas por las novedades tecnologicas.

Este entorno de trabajo permite la proactividad en cuanto a la rapidez de respuesta ante los nuevos riesgos relacionados con la IoT, la solución es proporcionada por la entidad capacitada para ello. La disminución de riesgos para las empresas representaría una oportunidad para desarrollar nuevos productos y servicios.

El engranaje entre los intereses empresariales con los de los usuarios, puede colisionar. Esta colisión de intereses debe ser resuelta en base a la legislación vigente, por lo que la participación de las áreas de negocio, jurídica y tecnológica evita problemas futuros.

La decisión final de las soluciones de privacidad, actualmente la realizan los expertos en seguridad, que en muchas ocasiones no son independientes de los intereses del promotor del servicio, la colaboración en el proceso del ámbito legal, ofrece garantías. Esta colaboración impulsará la emisión de certificaciones que darán garantía necesaria a usuarios y empresas, para minimizar los riesgos que se han estudiado en el estado del arte.

En el estado actual tecnológico, el hecho de ofrecer una seguridad a medida, ni más ni menos que la necesaria, proporciona el ahorro de recursos, necesario para no poner en riesgo la calidad del servicio.

Se demostrado que las necesidades de protección de datos personales no sólo se asocian al servicio final, sino al caso de uso y al tipo de usuario.

5.2. Beneficios del sistema

Este método de afrontar la seguridad y privacidad posibilita especificar solamente los servicios y mecanismos necesarios, en lugar de proporcionar todos por defecto, mejorando así la política de privacidad, con la mayor eficiencia en recursos. Este ahorro de recursos se puede calcular mediante el modelo matemático propuesto en el apartado 3.5.4 referente al ahorro de costes que sirve para calcular el ahorro en materia de seguridad, en función de la cantidad de servicios de seguridad no necesarios, y que por tanto no se proporcionan.

La garantía de que el servicio final ofrecido se adecúa a lo que marca la ley, si es avalado por el área jurídica (participando en el proceso), tiene una credibilidad mayor que la que pueden ofrecer los criterios de los expertos técnicos en seguridad, por buenos que estos sean. El aval jurídico como garantía, elimina riesgos transformando estas amenazas en oportunidades.

La diversidad de los puntos de vista de cada una de las áreas implicadas enriquece la visión del conjunto. De esta manera se puede apreciar que la determinación de los servicios y mecanismos de seguridad no solo debe de enfocarse en función aplicación, sino también del entorno y del usuario final.

Se pueden hacer simulaciones en dos ámbitos:

1.- Proporcionando la posibilidad de realizar estudios de costes por parte de las empresas y ensayar ideas de nuevos productos, antes de iniciar el proceso de desarrollo de un servicio.

2.- Permitiendo realizar ensayos para analizar el impacto que tendría una determinada modificación en la legislación que afecta a la privacidad. Se podría llegar hasta el punto de valorar el impacto económico que tendría el hecho de añadir, suprimir o modificar nuevas protecciones a los servicios finales que ya están funcionando.

Este sistema ofrece una base de conocimientos capaz de gestionar la gran cantidad de mecanismos existentes, y los que se van desarrollando, de forma que se clarifique su aplicabilidad, de forma que buenos mecanismos no pasen

desapercibidos. Hay una gran cantidad de métodos y esquemas de seguridad y privacidad aplicables a una gran variedad de tipos de redes y situaciones.

Facilita la realización y gestión eficiente de las actualizaciones o adaptaciones a los niveles de seguridad y privacidad que se necesitan en cada momento ante cambios sobrevenidos.

Se brinda la posibilidad de valorar el grado del cumplimiento de la legislación de protección de datos que tiene un servicio, un conjunto de servicios o una ciudad inteligente entera.

5.3. Cumplimiento de los objetivos

En cuanto a la transferencia de conocimientos generados por la actividad investigadora de esta tesis, se han realizado 6 publicaciones a las que se puede acceder mediante los enlaces [http://dx.doi.org/[seguido de DOI].

Jose-Antonio Sanchez-Alcon, Lourdes Lopez-Santidrian, and Jose-Fernan Martinez, “Solution to ensure privacy in the Internet of things,” Profesional De La Informacion, vol. 24, no. 1, pp. 62–70, 2015. http://dx.doi.org/10.3145/epi.2015.ene.08

Pedro Castillejo, José-Fernán Martínez-Ortega, Lourdes López, and **José Antonio Sánchez Alcón**, “SensoTrust: Trustworthy Domains in Wireless Sensor Networks,” International Journal of Distributed Sensor Networks, vol. 2015, Article ID 484820, 10 pages, 2015. http://dx.doi.org/10.1155/2015/484820

Sánchez Alcón, José A.; López, Lourdes; Martínez, José-Fernán; Rubio Cifuentes, Gregorio. 2016. "Trust and Privacy Solutions Based on Holistic Service Requirements." Sensors 16, no. 1: 16, 38 pages, 2016. http://dx.doi.org/10.3390/s16010016

Sanchez Alcon, J.A.; Lopez, L.; Martinez, J.-F.; Castillejo, P., "Automated determination of security services to ensure personal data protection in the Internet of Things applications," In Proceedings of the Innovative Computing Technology (INTECH), 2013 Third International Conference on , vol., no., pp.71-76, 29-31 Aug. 2013. http://dx.doi.org/10.1109/INTECH.2013.6653704. Congreso IEEE, publicado en WoS

Alcón, J.; López, L.; Martínez, J.; Castillejo, P. “Automatic System for Providing Security Services in the Internet of Things applications over Wireless Sensor Networks”. In Proceedings of the 1st Int. Electron. Conf. Sens. Appl., 1–16 June 2014; Sciforum Electronic Conference Series, Vol. 1, 2014 http://dx.doi.org/10.3390/ecsa-1-d005

Alcón, J.; Castillejo, P.; Martínez, J.; López, L. Firefighter and victims protecting solution based on Wireless Body Area Network nodes. In Proceedings of the 2nd Int. Electron. Conf. Sens. Appl., 15–30 November 2015; Sciforum Electronic Conference Series, Vol. 2, 2015 http://dx.doi.org/10.3390/ecsa-2-E012

En cuanto al objetivo general de esta tesis, se ha propuesto el sistema experto expuesto. Respecto a los objetivos específicos se ha analizado el entorno de negocio para determinar que la Matriz de Utilidad representa la entrada la información de entrada que se debe recopilar del promotor para su tratamiento por el sistema. Por otra parte el sistema ofrece a todas las áreas, la información necesaria en base a los indicadores definidos como KPI en el capítulo 3, para establecer sus planes de mejora continua. Se han determinado los imperativos legales y se ha llegado a la conclusión de que el mejor formato de presentación es el DPIA-T, y que se debe confeccionar tanto para los servicios individuales como para el servicio combinado que se preste en base a servicios individuales. Se ha propuesto una estructura de selección de los mecanismos basada en los ataques y contramedidas que afectan al tipo de red en concreto.

5.4. Trabajos futuros

Como se comentó al principio de este capítulo, se ha podido apreciar que realmente existe un interés por la idea de éste tipo de colaboración entre áreas, y la

percepción general es positiva. Actualmente existen muchas barreras de escepticismo. Debido a este escepticismo como contrapunto del interés producido, la primera actividad si se quiere implantar esta idea, es desarrollar una estrategia para eliminar estas barreras e iniciar este tipo de colaboración.

En el corto plazo, se debería establecer un foro de trabajo entre las tres áreas. Para ello se buscará la colaboración y participación de las universidades de derecho (cátedras relacionadas con los “sistemas expertos en el ámbito del derecho”), con empresas líderes del sector de las telecomunicaciones, particularmente Telefónica y Vodafone por su vinculación con la UPM y con una importante actividad en el campo de la IoT. Por lo que sería conveniente incluir en el foro a agentes de la esfera política (nacional, autonómica, municipal).

Una vez configurado un proyecto multidisciplinar se buscará financiación y la forma de acometerlo dependerá del interés de los promotores, pero la idea inicial es que el proyecto se realice en base a hitos acumulativos, de forma que cada hito del proyecto proporcione una parte utilizable del producto final, que sea útil para las entidades promotoras del proyecto.

Finalmente la idea es ponerlo en explotación extendiéndolo desde el ámbito local, al ámbito nacional.

6 Referencias y tabla de acrónimos

6.1. Referencias bibliográficas

Se ha mantenido en lo posible el contenido de cada campo, tal y como han sido originalmente catalogados por los editores, en particular los autores.

[1] Pablo García-Mexía, "La Internet de las Cosas y sus repercusiones jurídicas. La ley en la Red,". Available: http://abcblogs.abc.es/ley-red/public/post/la-internet-de-las-cosas-y-sus-repercusiones-juridicas-15395.asp/.

[2] J. A. Sanchez Alcon, L. Lopez, J.-F. Martinez, and P. Castillejo, "Automated determination of security services to ensure personal data protection in the Internet of Things applications," presented at the Third International Conference on Innovative Computing Technology (INTECH 2013), London, 2013, pp. 71–76.

[3] J.-A. Sánchez-Alcón, L. López-Santidrián, and J.-F. Martínez, "Solución para garantizar la privacidad en Internet de las Cosas," *El profesional de la información*, vol. 24, no. 1, pp. 62–70, Jan. 2015.

[4] Nuria Cuadrado Gamarra, *Aplicación de los Sistemas Expertos al Campo del Derecho*. Madrid, España: Facultad de Derecho de la Universidad Complutense de Madrid (Servicio de Publicaciones), 2004.

[5] C. Stevens, V. Barot, and J. Carter, "The Next Generation of Legal Expert Systems - New Dawn or False Dawn?," in *Research and Development in Intelligent Systems XXVII*, M. Bramer, M. Petridis, and A. Hopgood, Eds. London: Springer London, 2011, pp. 439–452.

[6] M. Venkateswarlu Naik, "Building a Legal Expert System for Legal Reasoning in Specific Domain-A Survey," *International Journal of Computer Science and Information Technology*, vol. 4, no. 5, pp. 175–184, Oct. 2012.

[7] Dave Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Wjite Paper." Cisco Internet Business Solutions Group (IBSG), Apr-2011.

[8] Joseph Bradley, Jeff Loucks, James Macaulay, and Andy Noronha, "Internet of

Everything (IoE) Value Index How Much Value Are Private-Sector Firms Capturing from IoE in 2013? White Paper." Cisco, 2013.

[9] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, "Disruptive Technologies: Advances that will transform life, business, and the global economy." McKinsey Global Institute, May-2013.

[10] "Global Conference on Cybersapce 2015 CHAIR'S STATEMENT." 2015.

[11] Council of Europe Treaty Office (1981). pp 1-10, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. CETS No.108. Strasbourg." 28-Jan-1981.

[12] Unión Europea (1995). Diario oficial, n. L 282 de 23/11/1995, pp. 0031-0050, "Directiva 95/46/CE del Parlamento Europeo y del Consejo, 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos." 28-Oct-2015.

[13] Parlamento Europeo (2004). Diario oficial n. C 102E de 28.4.2004, pp. 147-153, "Resolución del Parlamento Europeo sobre el primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)." 2004.

[14] Comité Económico y Social Europeo (2009). Diario oficial, n. C 255, 22/09/2010, pp. 116-120, "Dictamen sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Internet de los objetos - Un plan de acción para Europa [COM(2009) 278 final]." 28-Oct-2015.

[15] Comisión Europea (2012)., "Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), n. 2012/0011/ COD, 25/01/2012." 28-Oct-2015.

[16] European Commission n. 14/EN WP 223, adopted on 16 September 2014, pp. 1-24, "Opinion 8/2014 on the on recent developments on the Internet of things."

2014.

[17] Comisión Europea (2014). Diario oficial, n. L 300, 18/10/2014, pp. 63-68, "Recomendación de la Comisión de 10 de octubre de 2014 relativa al modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente." 2014.

[18] Unión Internacional de Telecomunicaciones, "X.800 : Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT." 1991.

[19] Sunil Gupta, Harsh K Verma, and A L Sangal, "Security attacks & prerequisite for wireless sensor networks," *International Journal of Engineering and Advanced Technology (IJEAT)*, no. 5, pp. 558–566, 2013.

[20] Palafox-Maestre, luis E; García Macías, J. Antonio, "Security in wireless sensor networks," in *Handbook of Research on Wireless Security:*, Yan Zhang and M. Ma, Eds. IGI Global, 2008, pp. 547–564.

[21] "IEEE Website," Available: http://www.ieee.org/about/index.html.

[22] "IEEE 802.15.4 Website," Available: http://www.ieee802.org/15/pub/TG4.html.

[23] "The ZigBee Alliance Website," Available: http://www.zigbee.org/.

[24] "IETF Website," Available: http://www.ietf.org/about/.

[25] "IPv6 over Low power WPAN (6lowpan) ," Available: http://datatracker.ietf.org/wg/6lowpan/charter/.

[26] "Routing Over Low power and Lossy networks (roll)," Available: http://datatracker.ietf.org/wg/roll/charter/.

[27] "Bluetooth SIG Website," Available: http://www.bluetooth.com/Pages/about-bluetooth-sig.aspx.

[28] "The Internet of Things is powered by Z-Wave.," Available: http://www.z-wavealliance.org.

[29] "Technology & Market overview: Sensing, monitoring and control solutions."

Available: ftp://ftp.cordis.europa.eu/pub/ist/docs/embedded/modjeska-280307_en.pdf

[30] "IEEE SA - 802.15.4-2006," *IEEE Standard Association*. Available: https://standards.ieee.org/findstds/standard/802.15.4-2006.html.

[31] C. Bormann, D. Sturek, and Z. Shelby, "6LowApp: Problem Statement for 6LoWPAN and LLN Application Protocols." draft-bormann-6lowpan-6lowapp-problem-00, 2009.

[32] "Bluetooth Technology Website," Available: http://www.bluetooth.com/Pages/PageNotFoundError.aspx?requestUrl=http://www.bluetooth.com/Bluetooth/SIG/.

[33] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Std 802.15.4-2003*, pp. 1–670, 2003.

[34] J. Daemen and V. Rijmen, "The Block Cipher Rijndael," in *Smart Card Research and Applications*, vol. 1820, J.-J. Quisquater and B. Schneier, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 277–284.

[35] M. Bellare, J. Kilian, and P. Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code," *Journal of Computer and System Sciences*, vol. 61, no. 3, pp. 362–399, Dec. 2000.

[36] D. Whiting, R. Housley, and N. Ferguson, "RFC 3610 - Counter with CBC-MAC (CCM)." 2003.

[37] ZigBee Alliance, "ZigBee Specification ", r17 version." ZigBee Standards Organization, 2008.

[38] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," presented at the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc

Communications and Networks, IEEE SECON 2004. 2004, Santa Clara, California, 2004, pp. 71–80.

[39] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 26, no. 1, pp. 96–99, Jan. 1983.

[40] David W. Carman, Peter S. Kruus, and Brian J. Matt, "Constraints and approaches for distributed sensor network security," *Technical Report 00-010, NAI Labs, Network Associates Inc.*, no. 2000.

[41] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," in *Cryptographic Hardware and Embedded Systems - CHES 2004*, vol. 3156, M. Joye and J.-J. Quisquater, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 119–132.

[42] G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public Key Cryptography in Sensor Networks—Revisited," in *Security in Ad-hoc and Sensor Networks*, vol. 3313, C. Castelluccia, H. Hartenstein, C. Paar, and D. Westhoff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 2–18.

[43] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and Sheueling Chang Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," presented at the Third IEEE International Conference on Pervasive Computing and Communication PerCom 2005., 2005, pp. 324–328.

[44] Burt Kaliski, "RSA Laboratories - TWIRL and RSA Key Size." 06-May-2003.

[45] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," presented at the Ninth international conference on Architectural support for programming languages and operating systems (ASPLOS IX), 2000, pp. 93–104.

[46] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, vol. 19964964. CRC Press, 1996.

[47] R. L. Rivest, "The RC5 encryption algorithm," in *Fast Software Encryption*, vol.

1008, B. Preneel, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 86–96.

[48] D. Eastlake and P. Jones, “RFC 3174 - US Secure Hash Algorithm 1 (SHA1).” 2001.

[49] R. Rivest, “RFC 1321. The MD5 Message-Digest Algorithm.” Apr-1992.

[50] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, “Analyzing and modeling encryption overhead for sensor network nodes,” presented at the 2nd ACM international conference on Wireless sensor networks and applications (WSNA ’03), 2003, p. 151.

[51] R. Stoleru, T. He, J. A. Stankovic, and D. Luebke, “A high-accuracy, low-cost localization system for wireless sensor networks,” presented at the 3rd international conference on Embedded networked sensor systems (SenSys ’05), 2005, p. 13.

[52] J. R. Douceur, “The Sybil Attack,” in *Peer-to-Peer Systems*, vol. 2429, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 251–260.

[53] J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: analysis & defenses,” presented at the 3rd international symposium on Information processing in sensor networks (IPSN ’04), 2004, pp. 259–268.

[54] Haowen Chan and A. Perrig, “Security and privacy in sensor networks,” *IEEE Computer Magazine*, vol. 36, no. 10, pp. 103–105, Oct. 2003.

[55] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[56] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[57] M. Sethi, J. Arkko, and A. Keranen, “End-to-end security for sleepy smart object networks,” presented at the IEEE 37th Conference on Local Computer Networks

Workshops (LCN Workshops 2012), Clearwater, FL, 2012, pp. 964–972.

[58] David W. Carman, Peter S. Kruus, and Brian J. Matt, "Constraints and approaches for distributed sensor network security (final)." NAI Labs Technical Report #00-010, 2000.

[59] Haowen Chan, Adrian Perrig, and Dawn Song, "Random key pre-distribution schemes for sensor networks," presented at the IEEE Symposium on Security and Privacy (SP '03), Washington, DC, USA, 2003, p. 197–.

[60] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 3–13, Jan. 2007.

[61] R. Di Pietro, L. V. Mancini, Yee Wei Law, S. Etalle, and P. Havinga, "LKHW: a directed diffusion-based secure multicast scheme for wireless sensor networks," presented at the International Conference on Parallel Processing Workshops, 2003., 2003, pp. 397–406.

[62] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," presented at the 10th ACM conference on Computer and communications security (CCS '03), Denver, Colorado, USA, 2003, p. 62.

[63] J. Lee and D. R. Stinson, "Deterministic Key Predistribution Schemes for Distributed Sensor Networks," in *Selected Areas in Cryptography*, vol. 3357, H. Handschuh and M. A. Hasan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 294–307.

[64] Jooyoung Lee and D. R. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks," presented at the IEEE Wireless Communications and Networking conference, 2005, vol. 2, pp. 1200–1205.

[65] Haowen Chan and Adrian Perrig, "PIKE: Peer intermediaries for key establishment in sensor networks," presented at the IEEE INFOCOM 2005 The 24th Annual Conference Sponsored by IEEE Communications Society, Miami, 2005, vol. 1, pp. 524–535.

[66] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," presented at the 2nd ACM International Conference on Wireless Sensor Networks and Applications, 2003, pp. 141-150.

[67] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," presented at the 9th ACM conference on Computer and communications security (CCS '02), 2002, p. 41.

[68] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security*, vol. 8, no. 2, pp. 228–258, May 2005.

[69] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 41–77, Feb. 2005.

[70] R. Di Pietro, L. V. Mancini, and A. Mei, "Random key-assignment for secure Wireless Sensor Networks," presented at the 1st ACM workshop on Security of ad hoc and sensor networks (SASN '03), 2003, p. 62.

[71] Wenliang Du, Jing Deng, Y. S. Han, Shigang Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," presented at the IEEE INFOCOM. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, Hong Kong, 2004, vol. 1, pp. 586–597.

[72] D. D. Hwang, B.-C. C. Lai, and I. Verbauwhede, "Energy-Memory-Security Tradeoffs in Distributed Sensor Networks," in *Ad-Hoc, Mobile, and Wireless Networks*, vol. 3158, I. Nikolaidis, M. Barbeau, and E. Kranakis, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 70–81.

[73] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," in *Advances in Cryptology — CRYPTO' 92*, vol. 740, E. F. Brickell, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 471–486.

[74] Papadimitratos, Panos and Haas, Z. J., "Secure routing for mobile ad hoc networks," presented at the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, 2002, pp. 193–204.

[75] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," presented at the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), Washington, DC, USA, 2004, p. 43.

[76] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, Dec. 2004.

[77] C. Li, H. Zhang, B. Hao, and J. Li, "A Survey on Routing Protocols for Large-Scale Wireless Sensor Networks," *Sensors*, vol. 11, no. 12, pp. 3498–3526, Mar. 2011.

[78] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," presented at the 6th annual international conference on Mobile computing and networking (MobiCom '00), 2000, pp. 243–254.

[79] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," presented at the First IEEE International Workshop onSensor Network Protocols and Applications, 2003, pp. 113–127.

[80] B. Przydatek, D. Song, and A. Perrig, "SIA: secure information aggregation in sensor networks," presented at the 1st international conference on Embedded networked sensor system (SenSys '03), 2003, pp. 255–265.

[81] Dongang Liu and Peng Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks," presented at the 10th Annual Network and Distributed System Security Symposium, San Diego, CA, 2003, pp. 263–276.

[82] D. Liu and P. Ning, "Multilevel μTESLA: Broadcast authentication for distributed sensor networks," *ACM Transactions on Embedded Computing Systems*, vol. 3, no. 4, pp. 800–836, Nov. 2004.

[83] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor netowrks," presented at the 7th annual international conference on Mobile computing and networking (MobiCom '01), Rome, Italy, 2001, pp. 189–199.

[84] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, no. 2, pp. 216–230, Jan. 2006.

[85] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Poster abstract secure locations: routing on trust and isolating compromised sensors in location-aware sensor networks," presented at the 1st International Conference on Embedded Networked Sensor Systems, 2003, pp. 324–325.

[86] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A witness-based approach for data fusion assurance in wireless sensor networks," presented at the IEEE Global Telecommunications Conference, 2003. GLOBECOM '03, 2003, vol. 3, pp. 1435–1439.

[87] B. Parno, A. Perrig, and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," presented at the IEEE Symposium on Security and Privacy, 2005, 2005, pp. 49–63.

[88] David Braginsky, "Rumor routing algorithm for sensor networks," presented at the 1 ACM International Workshop on Wireless Sensor Networks and Applications, New York, NY, USA, 2002, pp. 22–31.

[89] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: scalable coordination in sensor networks," presented at the 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom '99), 1999, pp. 263–270.

[90] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TAG: a Tiny AGgregation service for ad-hoc sensor networks," *ACM SIGOPS Operating Systems Review*, vol. 36, no. SI, p. 131, Dec. 2002.

[91] Lingxuan Hu and D. Evans, "Secure aggregation for wireless networks,"

presented at the Symposium on Applications and the Internet Workshops, 2003, pp. 384–391.

[92] Hasan Cam, Suat Ozdemir, H. Ozgur Sanli, and Prashant Nair, "Secure Differential Data Aggregation for Wireless Sensor Networks," in *Sensor Network Operations*, Wiley-IEEE Press, 2004, pp. 422–441.

[93] H. Cam, S. Ozdemir, P. Nair, and D. Muthuavinashiappan, "ESPDA: Energy-efficient and Secure Pattern-based Data Aggregation for wireless sensor networks," presented at the IEEE Sensors, 2003., 2003, vol. 2, pp. 732–736.

[94] H. Cam, S. Ozdemir, D. Muthuavinashiappan, and P. Nair, "Energy efficient security protocol for wireless sensor networks," presented at the IEEE 58th Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003, 2003, vol. 5, pp. 2981–2984.

[95] J. Domingo-Ferrer, "A Provably Secure Additive and Multiplicative Privacy Homomorphism*," in *Information Security*, vol. 2433, A. H. Chan and V. Gligor, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 471–483.

[96] D. Wagner, "Cryptanalysis of an Algebraic Privacy Homomorphism," in *Information Security*, vol. 2851, C. Boyd and W. Mao, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 234–239.

[97] J. Girao, D. Westhoff, and M. Schneider, "CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks," presented at the IEEE International Conference on Communications, 2005. ICC 2005, 2005, vol. 5, pp. 3044–3049.

[98] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," presented at the The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services. MobiQuitous 2005., 2005, pp. 109–117.

[99] V. C. Gungor and G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[100] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[101] Srinivasan, A and Wu, J., "A survey on secure localization in wireless sensor networks.," in *Encyclopedia of Wireless and Mobile communications.*, B. Furht, 2008.

[102] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," presented at the 1st international conference on Mobile systems, applications and services (MobiSys '03), 2003, pp. 31–42.

[103] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, "Privacy-aware location sensor networks," presented at the 9th USENIX Workshop on Hot Topics in Operating Systems, (HotOS IX), 2003, vol. 3, pp. 163–168.

[104] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket location-support system," presented at the 6th annual international conference on Mobile computing and networking (MobiCom '00), 2000, pp. 32–43.

[105] A. Smailagic and D. Kogan, "Location sensing and privacy in a context-aware computing environment," *IEEE Wireless Communications*, vol. 9, no. 5, pp. 10–17, Oct. 2002.

[106] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[107] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," presented at the 6th annual international conference on Mobile computing and networking (MobiCom '00), 2000, pp. 255–265.

[108] Yongguang Zhang, Wenke Lee, and Yi-An Huang, "Intrusion detection techniques for mobile wireless networks," *Wireless Networks*, vol. 9, no. 5, pp. 545–556, Sep. 2003.

[109] Y. Huang and W. Lee, "Attack Analysis and Detection for Ad Hoc Routing Protocols," in *Recent Advances in Intrusion Detection*, vol. 3224, E. Jonsson, A.

Valdes, and M. Almgren, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 125–145.

[110] Sencun Zhu, S. Setia, S. Jajodia, and Peng Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," presented at the IEEE Symposium on Security and Privacy, Oakland, CA, 2004, pp. 259–271.

[111] Guiling Wang, Wensheng Zhang, Guohong Cao, and T. La Porta, "On supporting distributed collaboration in sensor networks," presented at the Military Communications Conference, 2003. MILCOM '03, 2003, vol. 2, pp. 752–757.

[112] Patrick Albers, Olivier Camp, Jean-marc Percher, Bernard Jouga, and Ricardo Puttini, "Security in ad hoc networks: A general intrusion detection architecture enhancing trust-based approaches," presented at the First International Workshop on Wireless Information Systems (WIS-2002), 2002, pp. 1–12.

[113] Asad Amir Pirzada and Chris McDonald, "Establishing trust in pure ad-hoc networks," presented at the 27th Australasian conference on Computer, Dunedin, New Zealand, 2004, vol. 26, pp. 47–54.

[114] A. Oram, Ed., *Peer-to-peer: harnessing the benefits of a disruptive technology*, 1st ed. Beijing ; Sebastopol, CA: O'Reilly & AssociatesO'Reilly, 2001.

[115] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," presented at the 7th Nordic Workshop on Secure IT Systems (NordSec'03), 2003, pp. 1–14.

[116] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim, "Highly reliable trust establishment scheme in ad hoc networks," *Computer Networks*, vol. 45, no. 6, pp. 687–699, Aug. 2004.

[117] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," presented at the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), Washington, DC, USA, 2004, p. 66.

[118] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Location-centric

isolation of misbehavior and trust routing in energy-constrained sensor networks," presented at the IEEE International Conference on Performance, Computing, and Communications, 2004, pp. 463–469.

[119] Zhengqiang Liang and Weisong Shi, "PET: A PErsonalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing," presented at the 38th Annual Hawaii International Conference HICSS '05, 2005, p. 201b–201b.

[120] T. Aura, P. Nikander, and J. Leiwo, "DOS-Resistant Authentication with Client Puzzles," in *Security Protocols*, vol. 2133, B. Christianson, J. A. Malcolm, B. Crispo, and M. Roe, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 170–177.

[121] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," presented at the IEEE Computer and Communications Societies (INFOCOM'03), San Francisco, California, USA., 2003, vol. 3, pp. 1976–1986.

[122] Lingxuan Hu and David Evans, "Using directional antennas to prevent wormhole attacks," presented at the 11th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, 2004, pp. 1–11.

[123] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," presented at the 3rd ACM workshop on Wireless security (WiSe '04), Philadelphia, Pennsylvania, USA, 2004, pp. 51–60.

[124] Ross Anderson and Markus Kuhn, "Tamper Resistance - a Cautionary Note," presented at the 2nd USENIX Workshop on Electronic Commerce, Oakland, California, 1996, vol. 2, pp. 1–11.

[125] R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices," in *Security Protocols*, vol. 1361, B. Christianson, B. Crispo, M. Lomas, and M. Roe, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 125–136.

[126] Oliver Kommerling and Markus G. Kuhn, "Design principles for tamper-resistant smart card processors," presented at the USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, 1999, pp. 9–20.

[127] J. Deng, R. Han, and S. Mishra, "Security, privacy, and fault tolerance in wireless sensor networks," *Artech House*, 2005.

[128] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," presented at the 2nd ACM workshop on Wireless security (WiSe '03), Pittsburgh, PA, 2003, pp. 1–10.

[129] X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii, "Search-based physical attacks in sensor networks: Modeling and defense. Technical report," presented at the International Conference on Computer Communications and Networks (ICCCN), Ohio State University, 2005.

[130] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT: software-based attestation for embedded devices," presented at the IEEE Symposium on Security and Privacy, 2004, 2004, pp. 272–282.

[131] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *ACM Computing Surveys*, vol. 35, no. 3, pp. 309–329, Sep. 2003.

[132] Loukas Lazos and Radha Poovendran, "Secure Broadcast in Energy-Aware Wireless Sensor Networks," presented at the IEEE International Symposium on Advances in Wireless Communications (ISWC'02), 2002.

[133] L. Lazos and R. Poovendran, "SeRLoc: Robust localization for wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 1, pp. 73–100, Aug. 2005.

[134] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," presented at the 6th annual international conference on Mobile computing and networking. MobiCom '00, 2000, pp. 56–67.

[135] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure multicast groups on ad hoc networks," presented at the 1st ACM workshop on Security of ad hoc and sensor networks (SASN '03), 2003, pp. 94–102.

[136] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J.-M. Tang, "Framework for security and privacy in automotive telematics," presented at the 2nd international workshop on Mobile commerce (WMC '02), 2002, p. 25.

[137] E. Snekkenes, "Concepts for personal location privacy policies," presented at the 3rd ACM conference on Electronic Commerce (EC '01), 2001, pp. 48–57.

[138] G. Myles, A. Friday, and N. Davies, "Preserving privacy in environments with location-based applications," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 56–64, Jan. 2003.

[139] U. Hengartner and P. Steenkiste, "Protecting Access to People Location Information," in *Security in Pervasive Computing*, vol. 2802, D. Hutter, G. Müller, W. Stephan, and M. Ullmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 25–38.

[140] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," presented at the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), 2004, pp. 88–93.

[141] Jing Deng, R. Han, and S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," presented at the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005), 2005, pp. 113–126.

[142] M. Dener, "Security Analysis in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2014, pp. 1–9, 2014.

[143] N. Fatema and R. Brad, "Attacks and Counterattacks on Wireless Sensor Networks," *International Journal of Ad hoc, Sensor & Ubiquitous Computing*, vol. 4, no. 6, pp. 1–15, Dec. 2013.

[144] H. Maw, H. Xiao, B. Christianson, and J. Malcolm, "A Survey of Access Control Models in Wireless Sensor Networks," *Journal of Sensor and Actuator Networks*, vol. 3, no. 2, pp. 150–180, Jun. 2014.

[145] Babli Kumari and Jyoti Shukla, "Secure routing in wireless sensor networks,"

Ijarcsse, vol. 3, no. 8, pp. 746–751, 2013.

[146] Jyoti Shukla and Babli Kumari, "Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview," *IJAIEM*, vol. 2, no. 3, pp. 165–175, 2013.

[147] N. Zaman, K. Ragab, and A. B. Abdullah, Eds., *Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management*. IGI Global, 2012.

[148] Kutadi Venu Madhav, Rajendra C., and Raja Lakshmi Selvaraj, "A study of security challenges in wireless sensor networks," *JATIT*, vol. 20, no. 1, pp. 39–44, 2010.

[149] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 293–315, Sep. 2003.

[150] Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems. Smart Grid Task Force 2012-1." 2014.

[151] M. M. Islam, M. M. Hassan, G.-W. Lee, and E.-N. Huh, "A Survey on Virtualization of Wireless Sensor Networks," *Sensors*, vol. 12, no. 12, pp. 2175–2207, Feb. 2012.

[152] M. M. Islam and E.-N. Huh, "Virtualization in Wireless Sensor Network: Challenges and Opportunities," *Journal of Networks*, vol. 7, no. 3, pp. 412–418, Mar. 2012.

[153] N. Martínez, J.-F. Martínez, and V. Hernández Díaz, "Virtualization of Event Sources in Wireless Sensor Networks for the Internet of Things," *Sensors*, vol. 14, no. 12, pp. 22737–22753, Dec. 2014.

[154] M. S. Familiar, J. F. Martínez, and L. López, "Pervasive Smart Spaces and Environments: A Service-Oriented Middleware Architecture for Wireless Ad Hoc and Sensor Networks," *International Journal of Distributed Sensor Networks*,

vol. 2012, pp. 1–11, 2012.

[155] P. Castillejo, J.-F. Martínez-Ortega, L. López, and J. A. Sánchez Alcón, "SensoTrust: Trustworthy Domains in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2015, pp. 1–10, 2015.

[156] Alcón, J., Castillejo, P., Martínez, J., López, L. "Firefighter and victims protecting solution based on Wireless Body Area Network nodes". presented at the *2nd Int. Electron. Conf. Sens. Appl.*, 15–30 November 2015; Sciforum Electronic Conference Series, Vol. 2, 2015, E012; doi:10.3390/ecsa-2-E012

[157] A. R. Metke and R. L. Ekl, "Smart Grid security technology," presented at the Innovative Smart Grid Technologies (ISGT 2010), Gaithersburg, MD, 2010, pp. 1–7.

[158] D. Wu and C. Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 375–381, Jun. 2011.

[159] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[160] M. Nabeel, S. Kerr, Xiaoyu Ding, and E. Bertino, "Authentication and key management for Advanced Metering Infrastructures utilizing physically unclonable functions," presented at the IEEE Third International Conference on Smart Grid Communications (SmartGridComm 2012), Tainan, 2012, pp. 324–329.

[161] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions," presented at the First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), Gaithersburg, MD, 2010, pp. 350–355.

[162] R. Berthier and W. H. Sanders, "Specification-Based Intrusion Detection for Advanced Metering Infrastructures," presented at the 17th Pacific Rim IEEE International Symposium on Dependable Computing (PRDC 2011), Pasadena, CA, 2011, pp. 184–193.

[163] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cardenas, and J. G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," presented at the IEEE Third International Conference on Smart Grid Communications (SmartGridComm), 2012., Tainan, 2012, pp. 395–400.

[164] Y.-J. Kim, M. Thottan, V. Kolesnikov, and W. Lee, "A secure decentralized data-centric information infrastructure for smart grid," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 58–65, Nov. 2010.

[165] J. Camenisch and A. Lysyanskaya, "A Signature Scheme with Efficient Protocols," in *Security in Communication Networks*, vol. 2576, S. Cimato, G. Persiano, and C. Galdi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 268–289.

[166] F. Skopik, Z. Ma, T. Bleier, and H. Grüneis, "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures," *International Journal of Smart Grid and Clean Energy*, pp. 22–28, 2012.

[167] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.

[168] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[169] F. M. Cleveland, "Cyber security issues for Advanced Metering Infrasttructure (AMI)," presented at the Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, Pittsburgh, PA, 2008, pp. 1–5.

[170] "White Paper for NIST CSWG: Cyber Security Requirements for Business Processes Involving Home Area Networks (HAN)." Xantus Consulting International, 2009.

[171] Yilin Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, Heejo Lee, A. Perrig, and B. Sinopoli, "Cyber-Physical Security of a Smart Grid Infrastructure," *Proceedings*

of the IEEE, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[172] Govindarasu, M., Hann, A., and Sauer, P., "Cyber-Physical Systems Security for Smart Grid Future Grid Initiative White Paper." PSERC Publication Iowa State University, 2012.

[173] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[174] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, May 2011.

[175] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," presented at the IEEE Global Communications Conference (GLOBECOM 2012), Anaheim, CA, 2012, pp. 3153–3158.

[176] S. Saponara and T. Bacchillone, "Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid," *Journal of Computer Networks and Communications*, vol. 2012, pp. 1–19, 2012.

[177] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure Lossless Aggregation for Smart Grid M2M Networks," presented at the First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), Gaithersburg, MD, 2010, pp. 333–338.

[178] F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," *International Journal of Security and Networks*, vol. 6, no. 1, p. 28, 2011.

[179] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, Aug. 2012.

[180] A. Lazakidou, K. Siassiakos, and K. Ioannou, Eds., *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*. IGI Global, 2011.

[181] T. Tsao, R. Alexander, M. Dohler, V. Daza, and A. Lozano, "A Security Framework for Routing over Low Power and Lossy Networks. IETF Std. ROLL, Work in progress." draft-ietf-roll-security-framework-07, 2012.

[182] P. M. Nasr and A. Y. Varjani, "Alarm based anomaly detection of insider attacks in SCADA system," presented at the Smart Grid Conference (SGC 2014), Tehran, 2014, pp. 1–6.

[183] Bonnie Zhu and Shankar Sastry, "SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy.," presented at the 1st Workshop on Secure Control Systems (SCS'10), 2010.

[184] P. M. Nasr and A. Y. Varjani, "Petri net model of insider attacks in SCADA system," presented at the 11th International ISC Conference on Information Security and Cryptology (ISCISC 2014), Tehran, 2014, pp. 55–60.

[185] Jacques Benoit, "An Introduction to Cryptography as Applied to the Smart Grid." Cooper Power Systems, 2011.

[186] M. M. Fouda, Z. M. Fadlullah, N. Kato, Rongxing Lu, and Xuemin Shen, "A Lightweight Message Authentication Scheme for Smart Grid Communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[187] X. Lu, W. Wang, and J. Ma, "Authentication and Integrity in the Smart Grid: An Empirical Study in Substation Automation Systems," *International Journal of Distributed Sensor Networks*, vol. 2012, pp. 1–13, 2012.

[188] Sushmita Ruj, Amiya Nayak, and Ivan Stojmenovic, "A Security Architecture for Data Aggregation and Access Control in Smart Grids," pp. 1–12, 2011.

[189] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for Smart Energy Home Area Networks," presented at the IEEE International Conference on Consumer Electronics (ICCE 2011), Las Vegas, NV, 2011, pp.

787–788.

[190] Jung, Markus, Kienesberger, Georg, Granzer, Wolfgang, Unger, Martin, and Kastner, Wolfgang, "Privacy enabled web service access control using SAML and XACML for home automation gateways," presented at the International Conference for Internet Technology and Secured Transactions (ICITST), 2011, Abu Dhabi, 2011, pp. 584 – 591.

[191] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI application and security for controlled home area networks," presented at the IEEE Power and Energy Society General Meeting, 2011, San Diego, CA, 2011, pp. 1–8.

[192] E.-K. Lee, S. Y. Oh, and M. Gerla, "Frequency quorum rendezvous for fast and resilient key establishment under jamming attack," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 14, no. 4, p. 1, Feb. 2011.

[193] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Securing Advanced Metering Infrastructure Using Intrusion Detection System with Data Stream Mining," in *Intelligence and Security Informatics*, vol. 7299, M. Chau, G. A. Wang, W. T. Yue, and H. Chen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 96–111.

[194] S. Uludag, S. Zeadally, and M. Badra, "Techniques, Taxonomy, and Challenges of Privacy Protection in the Smart Grid," in *Privacy in a Digital, Networked World*, S. Zeadally and M. Badra, Eds. Cham: Springer International Publishing, 2015, pp. 343–390.

[195] S. Bhattarai, L. Ge, and W. Yu, "A novel architecture against false data injection attacks in smart grid," presented at the IEEE International Conference on Communications (ICC), 2012, Ottawa, ON, 2012, pp. 907–911.

[196] Yi Huang, H. Li, K. A. Campbell, and Zhu Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test," presented at the 45th Annual Conference on Information Sciences and Systems (CISS 2011), Baltimore, MD, 2011, pp. 1–6.

[197] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, “Smart grid data integrity attacks: characterizations and countermeasures (pi),” presented at the IEEE International Conference on Smart Grid Communications (SmartGridComm 2011), Brussels, 2011, pp. 232–237.

[198] Zhifeng Xiao, Yang Xiao, and D. H.-C. Du, “Non-repudiation in neighborhood area networks for smart grid,” *IEEE Communications Magazine*, vol. 51, no. 1, pp. 18–26, Jan. 2013.

6.2. Tabla de enlaces.

Ref.	Enlace	Enlace alternativo [http://dx.doi.org/[seguido de DOI]
1	http://abcblogs.abc.es/ley-red/public/post/la-internet-de-las-cosas-y-sus-repercusiones-juridicas-15395.asp/	
2	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6653704	10.1109/INTECH.2013.6653704
3	http://recyt.fecyt.es/index.php/EPI/article/view/epi.2015.ene.08	10.3145/epi.2015.ene.08
5	http://link.springer.com/10.1007/978-0-85729-130-1_33	
6	http://www.airccse.org/journal/jcsit/4512ijcsit14.pdf	10.5121/ijcsit.2012.4514
7	http://es.ptc.com/File%20Library/Topics/Smart%20Connected%20Products/IoT_IBSG_NextEvolutionoftheInternet.pdf	
8	http://es.ptc.com/File%20Library/Topics/Smart%20Connected%20Products/Internet_of_Everything_Value_Index_Whitepaper.pdf	
9	http://es.ptc.com/File%20Library/Topics/Smart%20Connected%20Products/MGI_Disruptive_Technologies_Full_Report_May2013.pdf	
10	https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf	
11	http://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/108	
12	http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L:1995:282:TOC	
13	http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52004IP0141&qid=1420387565870	
14	http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52009AE1951&qid=1420395947268	
15	http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012PC0011&qid=1420389265736	
16	http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf	
17	http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014H0724&qid=1420390252490	
18	http://www.itu.int/rec/T-REC-X.800-199103-I/es	
19	http://www.ijeat.org/attachments/File/v2i5/E1809062513.pdf	
20	http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-59904-899-4	
21	http://www.ieee.org/about/index.html	
22	http://www.ieee802.org/15/pub/TG4.html	
23	http://www.zigbee.org/	
24	http://www.ietf.org/about/	
25	http://datatracker.ietf.org/wg/6lowpan/charter/	
26	http://datatracker.ietf.org/wg/roll/charter/	
27	http://www.bluetooth.com/Pages/about-bluetooth-sig.aspx	
28	http://www.z-wavealliance.org	
29	ftp://ftp.cordis.europa.eu/pub/ist/docs/embedded/modjeska-280307_en.pdf	
30	https://standards.ieee.org/findstds/standard/802.15.4-2006.html	
31	https://tools.ietf.org/html/draft-bormann-6lowpan-6lowapp-problem-00	
32	http://www.bluetooth.com/Pages/PageNotFoundError.aspx?requestUrl=http://www.bluetooth.com/Bluetooth/SIG/	
33	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1237559&isnumber=27762	10.1109/IEEESTD.2003.94389
34	http://link.springer.com/10.1007/10721064_26	

35	http://linkinghub.elsevier.com/retrieve/pii/S002200009991694X	10.1006/jcss.1999.1694
36	https://tools.ietf.org/html/rfc3610	
37	http://home.deib.polimi.it/cesana/teaching/IoT/papers/ZigBee/ZigBeeSpec.pdf	
38	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1381904	10.1109/SAHCN.2004.1381904
39	http://portal.acm.org/citation.cfm?doid=357980.358017	10.1145/357980.358017
40	http://www.csee.umbc.edu/courses/graduate/CMSC691A/Spring04/papers/nailabs_report_00-010_final.pdf	
41	http://link.springer.com/10.1007/978-3-540-28632-5_9	
42	http://link.springer.com/10.1007/978-3-540-30496-8_2	
43	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1392772	10.1109/PERCOM.2005.18
44	http://www.emc.com/emc-plus/rsa-labs/historical/twirl-and-rsa-key-size.htm	
45	http://portal.acm.org/citation.cfm?doid=378993.379006	10.1145/378993.379006
46	http://www.crcnetbase.com/doi/book/10.1201/9781439821916	
47	http://link.springer.com/10.1007/3-540-60590-8_7	
48	https://tools.ietf.org/html/rfc3174	
49	https://www.ietf.org/rfc/rfc1321.txt	
50	http://portal.acm.org/citation.cfm?doid=941350.941372	10.1145/941350.941372
51	http://portal.acm.org/citation.cfm?doid=1098918.1098921	10.1145/1098918.1098921
52	http://link.springer.com/10.1007/3-540-45748-8_24	
53	http://portal.acm.org/citation.cfm?doid=984622.984660	10.1145/984622.984660
54	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1236475	10.1109/MC.2003.1236475
55	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1055638	10.1109/TIT.1976.1055638
56	http://portal.acm.org/citation.cfm?doid=359340.359342	10.1145/359340.359342
57	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6424089	10.1109/LCNW.2012.6424089
58	http://www.csee.umbc.edu/courses/graduate/CMSC691A/Spring04/papers/nailabs_report_00-010_final.pdf	
60	http://linkinghub.elsevier.com/retrieve/pii/S1570870506000497	10.1016/j.adhoc.2006.05.014
61	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1240395	10.1109/ICPPW.2003.1240395
62	http://portal.acm.org/citation.cfm?doid=948109.948120	10.1145/948109.948120
63	http://link.springer.com/10.1007/978-3-540-30564-4_21	
64	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1424679	10.1109/WCNC.2005.1424679
65	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1497920&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1497920	10.1109/INFCOM.2005.1497920
66	http://portal.acm.org/citation.cfm?doid=941350.941371	10.1145/941350.941371
67	http://portal.acm.org/citation.cfm?doid=586110.586117	10.1145/586110.586117
68	http://portal.acm.org/citation.cfm?doid=1065545.1065548	10.1145/1065545.1065548
69	http://portal.acm.org/citation.cfm?doid=1053283.1053287	10.1145/1053283.1053287
70	http://portal.acm.org/citation.cfm?doid=986858.986868	10.1145/986858.986868
71	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1354530	10.1109/INFCOM.2004.1354530
72	http://link.springer.com/10.1007/978-3-540-28634-9_6	
73	http://link.springer.com/10.1007/3-540-48071-4_33	
74	http://kth.diva-portal.org/smash/record.jsf?pid=diva2%3A429037&dswid=-8204	

75	http://portal.acm.org/citation.cfm?doid=1029102.1029111	10.1145/1029102.1029111
76	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1368893	10.1109/MWC.2004.1368893
77	http://www.mdpi.com/1424-8220/11/4/3498/	10.3390/s110403498
78	http://portal.acm.org/citation.cfm?doid=345910.345953	10.1145/345910.345953
79	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1203362	10.1109/SNPA.2003.1203362
80	http://portal.acm.org/citation.cfm?doid=958491.958521	10.1145/958491.958521
81	http://www.internetsociety.org/doc/efficient-distribution-key-chain-commitments-broadcast-authentication-distributed-sensor	
82	http://portal.acm.org/citation.cfm?doid=1027794.1027800	10.1145/1027794.1027800
83	http://portal.acm.org/citation.cfm?doid=381677.381696	10.1145/381677.381696
84	http://linkinghub.elsevier.com/retrieve/pii/S0140366405002045	10.1016/j.comcom.2005.05.018
85	http://portal.acm.org/citation.cfm?doid=958491.958542	10.1145/958491.958542
86	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1258475	10.1109/GLOCOM.2003.1258475
87	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1425058	10.1109/SP.2005.8
88	http://research.cens.ucla.edu/people/estrin/resources/conferences/2002sept-Braginsky-Estrin-Rumor.pdf	
89	http://portal.acm.org/citation.cfm?doid=313451.313556	10.1145/313451.313556
90	http://portal.acm.org/citation.cfm?doid=844128.844142	10.1145/844128.844142
91	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1210191	10.1109/SAINTW.2003.1210191
92	http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.58.7205&rep=rep1&type=pdf	
93	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1279038	10.1109/ICSENS.2003.1279038
94	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1286170	10.1109/VETECF.2003.1286170
95	http://link.springer.com/10.1007/3-540-45811-5_37	
96	http://link.springer.com/10.1007/10958513_18	
97	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1494953	10.1109/ICC.2005.1494953
98	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1540992	10.1109/MOBIQUITOUS.2005.25
99	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4796311	10.1109/TIE.2009.2015754
100	http://linkinghub.elsevier.com/retrieve/pii/S1389128608001254	10.1016/j.comnet.2008.04.002
101	http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.86.3790&rep=rep1&type=pdf	
102	http://portal.acm.org/citation.cfm?doid=1066116.1189037	10.1145/1066116.1189037
103	https://www.usenix.org/legacy/events/hotos03/tech/full_papers/gruteser/gruteser_html/	
104	http://portal.acm.org/citation.cfm?doid=345910.345917	10.1145/345910.345917
105	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1043849	10.1109/MWC.2002.1043849
106	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1039518	10.1109/MC.2002.1039518
107	http://portal.acm.org/citation.cfm?doid=345910.345955	10.1145/345910.345955
108	http://link.springer.com/article/10.1023%2FA%3A1024600519144	10.1023/A:1024600519144
109	http://link.springer.com/10.1007/978-3-540-30143-1_7	
110	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1301328	10.1109/SECPRI.2004.1301328
111	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1290206	10.1109/MILCOM.2003.1290206
112	http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.103.9855	10.1.1.103.9855
113	http://dl.acm.org/citation.cfm?id=979929	
115	http://skirubame.ucoz.com/_ld/0/49_Trust_Evaluatio.pdf	
116	http://linkinghub.elsevier.com/retrieve/pii/S1389128604000714	10.1016/j.comnet.2004.01.008
117	http://portal.acm.org/citation.cfm?doid=1029102.1029115	10.1145/1029102.1029115
118	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1395061	10.1109/PCCC.2004.1395061
119	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1385650	10.1109/HICSS.2005.493
120	http://link.springer.com/10.1007/3-540-44810-1_22	
121	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1209219	10.1109/INFCOM.2003.1209219
122	http://www.cs.virginia.edu/~evans/pubs/ndss04.pdf	
123	http://portal.acm.org/citation.cfm?doid=1023646.1023657	10.1145/1023646.1023657
124	http://static.usenix.org/publications/library/proceedings/ec96/full_papers/kuhn/	
125	http://link.springer.com/10.1007/BFb0028165	
126	https://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf	
128	http://portal.acm.org/citation.cfm?doid=941311.941313	10.1145/941311.941313
129	http://citeseerx.ist.psu.edu/viewdoc/similar?doi=10.1.1.135.3316&type=sc	
130	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1301329	10.1109/SECPRI.2004.1301329

131	http://portal.acm.org/citation.cfm?doid=937503.937506	10.1145/937503.937506
132	http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA459885	
133	http://portal.acm.org/citation.cfm?doid=1077391.1077395	10.1145/1077391.1077395
134	http://portal.acm.org/citation.cfm?doid=345910.345920	10.1145/345910.345920
135	http://portal.acm.org/citation.cfm?doid=986858.986872	10.1145/986858.986872
136	http://portal.acm.org/citation.cfm?doid=570705.570711	10.1145/570705.570711
137	http://portal.acm.org/citation.cfm?doid=501158.501164	10.1145/501158.501164
138	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1186726	10.1109/MPRV.2003.1186726
139	http://link.springer.com/10.1007/978-3-540-39881-3_6	
140	http://portal.acm.org/citation.cfm?doid=1029102.1029117	10.1145/1029102.1029117
141	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1607564	10.1109/SECURECOMM.2005.16
142	http://www.hindawi.com/journals/ijdsn/2014/303501/	10.1155/2014/303501
143	http://www.airccse.org/journal/ijasuc/papers/4613ijasuc01.pdf	10.5121/ijasuc.2013.4601
144	http://www.mdpi.com/2224-2708/3/2/150/	10.3390/jsan3020150
145	http://www.ijarcsse.com/docs/papers/Volume_3/8_August2013/V3I6-0109.pdf	
146	http://www.ijaiem.org/Volume2Issue3/IJAIEM-2013-03-15-033.pdf	
147	http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-4666-0101-7	
148	http://www.jatit.org/volumes/research-papers/Vol20No1/5Vol20No1.pdf	
149	http://linkinghub.elsevier.com/retrieve/pii/S1570870503000088	10.1016/S1570-8705(03)00008-8
150	https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf	
151	http://www.mdpi.com/1424-8220/12/2/2175/	10.3390/s120202175
152	http://ojs.academypublisher.com/index.php/jnw/article/view/6972	10.4304/jnw.7.3.412-418
153	http://www.mdpi.com/1424-8220/14/12/22737/	10.3390/s141222737
154	http://www.hindawi.com/journals/ijdsn/2012/725190/	10.1155/2012/725190
155	http://www.hindawi.com/journals/ijdsn/2015/484820/	10.1155/2015/484820
156	http://sciforum.net/conference/ecsa-2/paper/3	10.3390/ecsa-2-E012
157	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5434760	10.1109/ISGT.2010.5434760
158	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5743049	10.1109/TSG.2011.2120634
159	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6805165	10.1109/COMST.2014.2320093
160	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6486004	10.1109/SmartGridComm.2012.6486004
161	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622068	10.1109/SMARTGRID.2010.5622068
162	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6133080	10.1109/PRDC.2011.30
163	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6486016	10.1109/SmartGridComm.2012.6486016
164	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5621968	10.1109/MCOM.2010.5621968
165	http://link.springer.com/10.1007/3-540-36413-7_20	
166	http://www.ijsgce.com/index.php?m=content&c=index&a=show&catid=27&id=16	10.12720/sgce.1.1.22-28
167	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6129371	10.1109/SURV.2011.122111.00145
168	http://linkinghub.elsevier.com/retrieve/pii/S1389128613000042	10.1016/j.comnet.2012.12.017
169	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4596535	10.1109/PES.2008.4596535
170	http://xanthus-consulting.com/Publications/documents/HAN_Business_Processes_Cyber_Security_Requirements.pdf	
171	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6016202	10.1109/JPROC.2011.2161428
172	http://www.pserc.wisc.edu/documents/publications/papers/fgwhitepapers/Govindarasu_Future_Grid_White_Paper_CPS_Feb2012.pdf	
173	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5963752	10.1109/TSG.2011.2159818
174	http://portal.acm.org/citation.cfm?doid=1952982.1952995	10.1145/1952982.1952995
175	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6503599	10.1109/GLOCOM.2012.6503599
176	http://www.hindawi.com/journals/jcnc/2012/534512/	10.1155/2012/534512
177	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622063	10.1109/SMARTGRID.2010.5622063
178	http://www.inderscience.com/link.php?id=39631	10.1504/IJSN.2011.039631
179	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6257525	10.1109/MCOM.2012.6257525
180	http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-61520-805-0	
181	https://tools.ietf.org/html/draft-ietf-roll-security-framework-07	

182	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7090881	10.1109/SGC.2014.7090881
183	http://www.cse.psu.edu/~sem284/cse598e-f11/papers/zhu.pdf	
184	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6994022	10.1109/ISCISC.2014.6994022
185	http://www.cooperindustries175.com/content/dam/public/powersystems/products/grid_automation/resources/Cryptography_and_the_Smart_Grid.pdf	
186	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5983424	10.1109/TSG.2011.2160661
187	http://www.hindawi.com/journals/ijdsn/2012/175262/	10.1155/2012/175262
188	http://arxiv.org/abs/1111.2619	
189	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5722864	10.1109/ICCE.2011.5722864
190	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6148403&isnumber=6148349	
191	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6038996	10.1109/PES.2011.6038996
192	http://portal.acm.org/citation.cfm?doid=1942268.1942270	10.1145/1942268.1942270
193	http://link.springer.com/10.1007/978-3-642-30428-6_8	
194	http://link.springer.com/10.1007/978-3-319-08470-1_15	
195	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6364511	10.1109/ICC.2012.6364511
196	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5766111	10.1109/CISS.2011.5766111
197	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6102324	10.1109/SmartGridComm.2011.6102324
198	http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6400434	10.1109/MCOM.2013.6400434

Tabla. 24. Enlaces a los documentos.

6.3. Acrónimos.

ACRÓNIMO	SIGNIFICADO
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks working group
ACL	Access Control List
ACK	Acknowledgement
AES	Advanced Encryption Standard
AES-CBC-MAC	Cipher Block Chaining - Message Authentication Code
AES- CCM	AES - Counter with CBC-MAC
AES-CTR	AES- Cipher Counter
AIMD	Adaptive Increase Multiplicative Decrease
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
APL	Application Layer
APS	APplication Support sub-layer
ASK	Amplitude Shift Keying
BT-LE	Bluetooth - Low Energy
CCM	Counter with Cipher block chaining-Message authentication code
CCM*	CCM variant
CCF	Congestion Control and Fairness
CSMA	Carrier Sense Multiple Access
CS	Carrier Sense
CSMA	Carrier Sense Multiple Access
CSMA/CA	CSMA with Collision Avoidance algorithm
CSMA/CD	CSMA with Collision Detection algorithm
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv6	IP version 6
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector
JSON	Java Script Object Notation
LAN	Local Area Network
LEACH	Low Energy Adaptive Clustering Hierarchy protocol
MicroTesla	Micro versión del timed Efficient Streaming LossTolerant
LoWPAN	Low power WPAN
KDC	Key Distribution Center
M2M	Machine to Machine
MAC	Medium Access Control layer
MAC	Message Authentication Code

ACRÓNIMO	SIGNIFICADO
NIST	National Institute of Standards and Technology
NWK	Network Layer
OS	Operating system
PAN	Personal Area Network
QoS	Quality of Service
RAM	Random Access Memory
RFID	Radio Frequency IDentification
RPL	IPv6 Routing Protocol for Low power and lossy networks
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition protocol
SKKE	Symmetric-Key-Key Establishment
SPIN	Sensor routing Protocols for Information via Negotiation
SQL	Structured Query Language
STCP	Sensor Transmission Control Protocol
TCP	Transmission Control Protocol
TDMA	Time Division Multiplex Access
TSMP	Time Synchronized Mesh Protocol
WPAN	Wireless Personal Area Networks
WSN	Wireless Sensor Network
XML	eXtensible Markup Language

Tabla. 25. Acrónimos utilizados en el documento.