

UNIVERSIDAD DE CANTABRIA

DEPARTAMENTO DE INGENIERÍA DE COMUNICACIONES



TESIS DOCTORAL

Contribución al diseño y evaluación de Redes Personales Cognitivas

Autor: *Jorge Lanza Calderón*

Director: *Luis Muñoz*

Santander, julio de 2014

Certificado del director de la tesis

D. Luis Muñoz, Catedrático de la Universidad de Cantabria en el Área de Ingeniería Telemática

HACE CONSTAR:

Que la tesis titulada “**Contribución al diseño y evaluación de Redes Personales Cognitivas**” ha sido realizada por **D. Jorge Lanza Calderón** en el Departamento de Ingeniería de Comunicaciones de la Universidad de Cantabria bajo mi dirección, y que reúne las condiciones exigidas a los trabajos de doctorado.

Santander, julio de 2014

Fdo. Luis Muñoz

*A mis padres,
a mi mujer y
a mi hijo*

Agradecimientos

Y como de bien nacido es ser agradecido, con la nostalgia de echar la vista atrás y tomar conciencia de lo mucho que ha acontecido, ha llegado el momento de escribir la parte que, aunque se considere la más sencilla, es posiblemente la que más cuesta.

Aún recuerdo el verano del año 2000 cuando tras una tarde de playa me acerqué al despacho de Luis Muñoz, uno de los profesores que por aquel entonces más respeto infundía en la carrera; la razón, conversar sobre la posibilidad de comenzar a trabajar en el Grupo de Ingeniería Telemática. Francamente, el respeto que ese día le tenía a Luis se ha acrecentado durante estos años, uniéndose a él la admiración por su esfuerzo, dedicación y tesón en la investigación. Gracias Luis, por guiar el tortuoso camino de esta tesis, pero sobre todo por estar ahí cuando se necesitaba tu apoyo y comprensión, y por esas conversaciones, tanto las serias como las distendidas.

Lo que presumiblemente iba a ser algo temporal, por circunstancias de la vida, se ha convertido en el día a día. Y los que iban a ser mis compañeros de trabajo, son hoy más que amigos; son casi una segunda familia.

Quiero acordarme primero de todos los que compartisteis conmigo jornadas en el Módulo 5. ¡Qué tiempos aquellos en el exilio! Juntos afrontamos el reto de hacer que en el grupo se hablara de algo más que de redes inalámbricas. Que sepáis que aún hoy se sigue hablando y mucho de la tarjeta inteligente. Óscar, Dulce, Ángel, Nacho, Carlos, Alejandra, Raquel, Satur, Marta y Pablo, de cada uno de vosotros guardo un recuerdo especial. Gracias por hacer que desde el principio venir a trabajar fuera un placer, por esas risas, por esas partiditas, . . . Prácticamente con todos vosotros sigo manteniendo contacto, así que aquí lo dejo por escrito: la siguiente corre de mi cuenta.

El resto no penséis que no me acuerdo de vosotros. Por gracia o por desgracia tengo que veros y sufriros cada día; y vosotros a mí. LSanchez, Ramón, Johnny, Jesús, Jose, Pablo y Carmen, David, Juanra, Luisco, Laura, Pablo, Javo, . . . para cada uno de vosotros solo tengo palabras de agradecimiento por haberme aguantado estoicamente durante este largo camino. Pablo, contigo he confirmado que la sangre puede ser realmente horchata, pero que aun así cuando hay que darlo todo siempre te vistes por los pies. Gracias por el apoyo en este último tramo. David, te lo dice uno que pensó que esto nunca se acababa: ¡ánimo que tus agradecimientos están un día más cerca! Y recuerda que la apuesta aún sigue en pie, aunque hay uno que ya no pierde, Jose. LSanchez, el dúo de trabajo quizás más dispar ha dado como resultado dos tesis. Gracias por tu apoyo. Es muy posible que nos queden muchos años juntos en el despacho, será un placer compartirlo contigo.

Mi agradecimiento también a los que forman parte del núcleo principal de la parte docente dentro del Grupo, Marta, Klaus, Jota, Rober y Alberto. En su momento me enseñasteis a mí y ahora juntos tenemos que hacer lo propio con las próximas generaciones.

No me he olvidado de ti Vero. Aunque formas parte del Grupo, sabes que significas mucho más. Para ti tengo un agradecimiento especial. Gracias por escucharme cuando se ha necesitado, por los consejos en los momentos difíciles, por hablar a veces más de la cuenta, . . . Gracias por ser como eres. Gracias por, en cierta manera, haber hecho posible que conociera a la persona con la que he formado una familia.

I would like to extend my gratitude to all the colleagues I have ever shared adventures with in any project I have worked. However, if I have a soft spot for one project, it is MAGNET. Not only has it provided the seed for this thesis, but also for many valued friendships. I doubt that I will ever work in a project like this one, where I have made so many good friends. I will never forget the endless integration meetings. Kimmo and Titta, Mikko, Sami, Juha, Jordi, Jeroen, Gerry, Rob, Ingrid, Djamal, Marc, . . . Hey guys, what about a beer afterwards! I would like to give my special thanks to the Finnish. You treated me as part of your family during my time there and that is something I will never forget. A little piece of me is and will always be Finnish.

Como no quiero dejarme a nadie en el tintero, mi más sincero agradecimiento a todos aquellos que de una u otra forma habéis compartido parte de este camino conmigo. A mi grupo de amigos, todos de una forma u otra habéis realizado vuestra aportación, animándome a continuar y a no tirar la toalla antes de finalizar el combate.

Y, por supuesto, el agradecimiento más profundo y sentido es para toda mi familia. Abuelos, Jero y Albino, gracias por seguir guiando mis pasos desde allí arriba. Mamá, te quiero. Gracias por, junto a papá, servirme de ejemplo y educarme de la manera que lo hicisteis. Si a alguien le debo gran parte de la persona que soy hoy, es a vosotros. Santi, papá, que sepas que siempre repaso contigo y allí donde voy te pongo como ejemplo de honestidad y generosidad.

Laura, a tu lado todo es más sencillo. Cada letra, cada palabra, cada frase, cada párrafo, cada capítulo; esta tesis no habría sido posible sin ti. Gracias por empujarme a seguir adelante, por evitar que me rinda, por aguantarme en los días malos y, sobre todo, por compartir cada día conmigo. Solo espero que exista el tiempo suficiente para devolverte al menos una parte de todo lo que me has dado. Eres mi mejor amiga y mi refugio. Por todo esto y mucho más, para ti el agradecimiento con mayúsculas ¡GRACIAS!

Y dejo para el final a lo mejor que me ha pasado en la vida, mi hijo Jonás. Gracias, porque una sonrisa tuya me alegra el día.

Jorge.

*Empieza haciendo lo necesario,
después lo posible,
y de repente te encontrarás haciendo lo imposible.*

San Francisco de Asís

Resumen

Transcurridos más de cincuenta años desde que se sembraran las primeras semillas que fructificarían en lo que hoy conocemos como sociedad de la información y las comunicaciones, se dispone de una visión histórica que permite afirmar sin ningún género de duda que en ese período gran parte de los esfuerzos llevados a cabo en términos de investigación, desarrollo e innovación han estado destinados a consolidar una infraestructura de comunicaciones masiva a nivel mundial que posibilite primeramente la comunicación entre las personas y posteriormente entre las máquinas, entendidas éstas en sentido amplio.

Es a comienzos del presente siglo cuando ese paradigma se desplaza hacia el individuo promoviendo nuevas tecnologías y servicios que facilitasen la comunicación de miríadas de dispositivos en torno al usuario con objeto de adquirir, procesar y decidir en cada momento las acciones más oportunas en base a diferentes consideraciones, como pueden ser el contexto o la privacidad. De esta forma se acuña el concepto de red de área personal, el cual se expande, de la mano de diferentes iniciativas, al de red personal y federación de redes personales. Términos como heterogeneidad y escalabilidad son inmanentes al concepto de federación de infraestructuras como se demuestra en la presente tesis aportando soluciones arquitecturales unificadas al efecto.

Previamente, partiendo de un conjunto de casos de uso suficientemente amplios se identifican los requerimientos funcionales que caracterizan de forma específica las necesidades de las redes personales y de su federación. Con objeto de conocer cuáles son los mecanismos que se han postulado para satisfacer dichos requerimientos se ha realizado el estudio del arte detallado tanto de la mano de acciones de estandarización como de proyectos internacionales de relieve.

Establecidos los requerimientos, se define el concepto de red personal (PN, *Personal Network*) del cual emana una concepción arquitectural basada en tres planos o capas: la capa de abstracción a nivel de conectividad, la de nivel de red y la de nivel de servicio. En la capa de abstracción a nivel de conectividad se examina la interconexión directa entre los dispositivos de usuario. Buscando dar respuesta a heterogeneidad en términos de tecnologías de acceso al medio, se define una capa universal de convergencia (UCL, *Universal Convergence Layer*), capaz de gestionar de forma inteligente los interfaces de acceso y aislar a las capas de comunicación superiores de la complejidad subyacente. La capa de abstracción a nivel de red considera los mecanismos de agrupación y comunicación de los nodos de una PN, sobre los que se sustenta el intercambio de datos de servicio. La capa de abstracción a nivel de servicio expone una plataforma distribuida de gestión que soporta la creación, publicación, descubrimiento y provisión de servicios.

En un plano ortogonal a las tres capas anteriores, se emplaza un plano destinado a la adquisición, gestión y provisión del contexto del usuario. El flujo de información a través de esta capa permitirá a las otras tres adaptar su operación en base a las necesidades específicas del usuario, su entorno y de otras PN que deseen interaccionar con aquélla.

Como también se desprende del análisis de los casos de uso, la seguridad en la PN juega un papel fundamental a la hora de motivar a los usuarios en la utilización de este tipo de infraestructuras. Así, con objeto de garantizar la privacidad, autenticidad y el no repudio de las comunicaciones se conciben y diseñan soluciones que hacen de la PN una red segura. Sustentada en la relación de propiedad existente entre los dispositivos de usuario y el propio usuario, se establecen los procedimientos para generar una relación bilateral de confianza entre los nodos de la PN. Este vínculo se propaga entre las diferentes capas de abstracción, lo que garantiza el intercambio seguro de información dentro de la PN.

Analizada la PN desde todos los niveles como entidad autónoma, se expande la PN con el concepto de federación de redes personales (PN-F, *Personal Networks Federation*) así como con una propuesta de diseño global de la arquitectura asociada. Considerando la PN-F como la agregación de PN que comparten recursos, se identifican eventuales nuevas entidades soportando funcionalidades añadidas o extendiendo las que emanan de las propias PN con objeto de integrarla en el marco de las PN-F. El planteamiento adoptado sigue dos aproximaciones: una que considera la PN-F como una agregación a nivel de red sobre la que se comparten todo tipo de recursos y otra en la que la agregación se realiza únicamente a nivel de servicio.

Más allá de la labor de especificación y diseño desarrollada en los primeros cinco capítulos del presente trabajo, se destina el capítulo 6 a validar en entornos de campo las diferentes soluciones propuestas. Para ello se emplea un demostrador distribuido en diferentes ubicaciones (París, Gante, Helsinki y Santander) sobre el que se analiza y evalúa el comportamiento y prestaciones de las diferentes soluciones adoptadas e implementadas.

Abstract

It is now more than fifty years since the first seeds were sown of what is now known as the Information and Communications Society. Historical vision allows us to state without any doubt that during this period much of the work done in terms of research, development and innovation efforts has been aimed at consolidating a massive, worldwide communications infrastructure that firstly made communication between people possible and later extended this to machines in their widest sense.

Early this century that paradigm shifted toward the individual, promoting new technologies and services that facilitated the communication of myriad user-centred devices in order to acquire, process and decide the appropriate action based on different considerations, such as the context or privacy. Thus, the concept of personal area network appeared which expanded, under different initiatives, to personal network and personal network federation. Terms such as heterogeneity and scalability are intrinsic to the concept of federation infrastructure as is demonstrated in this thesis, which provides architectural solutions unified for this purpose.

Previously, based on a sufficiently large set of usage cases, functional requirements were identified that specifically characterize the needs of personal networks and their federation. In order to elucidate the mechanisms that have been proposed to fulfil these requirements, a detailed study of the state-of-the-art has been carried out, both in relation to standardization activities and to significant international projects.

Once the requirements have been established, the concept of Personal Network (PN) is defined. Its architecture is based on three layers; an abstraction layer at the connectivity level, another at network level and another at service level. In the connectivity level abstraction layer, the direct interconnection among user devices is examined. In order to address heterogeneity in terms of medium access technologies, an Universal Convergence Layer (UCL) is defined, which can intelligently manage the access interfaces and isolate the upper communication layers from the underlying complexity. The network level abstraction layer deals with the mechanisms for grouping and communication of the nodes in a PN, on which the service's data exchange is based. The service level abstraction layer provides a distributed management platform that supports the creation, publication, discovery and provision of services.

Orthogonally to the above three layers, another layer was proposed for the acquisition, management and delivery of the user context. The information flow through this layer will allow the other three to adapt their operation based on the specific user needs, the environment and other PNs wishing to interact with it.

As can also be understood from the analysis of the usage cases, security in the PN plays a key role in motivating users in the use of this type of infrastructure. Thus, to ensure privacy, authenticity and non-repudiation of communications, strategies are conceived and designed to make the PN a secure network. Supported by the existing ownership relationship between user devices and the users themselves, procedures are established for generating a bilateral trust relationship between nodes of the PN. This bond is propagated throughout the different abstraction layers, ensuring the secure exchange of information within the PN.

Once the PN had been analysed from all levels as an autonomous entity, the PN was expanded with the concept of Personal Networks Federation as well as with a global design proposal of its associated architecture. Considering the PN-F as the aggregation of PNs that share resources, new entities were identified supporting added functionalities or extending those originating in the PNs in order to integrate them into the PN-F framework. The approach follows two approximations: one that considers the PN-F as an aggregation at the network level on which all types of resources are shared and another in which the aggregation is performed only at service level.

As an extension to the specification and design work described in the first five chapters of this thesis, Chapter 6 is intended to validate the different solutions proposed in field environments. This required a demonstrator distributed in different locations (Paris, Ghent, Helsinki and Santander) on which the behaviour and performance of the different solutions adopted and implemented was analysed and evaluated.

Índice

Índice de figuras	XIX
Índice de tablas	XXIII
Índice de cuadros de texto	XXV
Lista de acrónimos	XXVII
1 Introducción	1
1.1. Motivación y objetivos	3
1.2. Estructura de la tesis	4
2 Requerimientos e iniciativas relacionadas	7
2.1. Escenarios y casos de uso	7
2.1.1. Cuidado remoto de niños	7
2.1.2. Ejecutiva del mercado de valores	8
2.1.3. Viaje de trabajo	8
2.1.4. Vendedor ambulante	9
2.2. Requerimientos de una red personal	9
2.2.1. Facilidad de uso	10
2.2.2. Seguridad, confianza y privacidad	11
2.2.3. Comunicaciones ubicuas	13
2.2.4. Gestión y provisión de servicios	14
2.2.5. Adaptabilidad al contexto	15
2.3. Requerimientos de una federación de redes personales	15
2.4. Iniciativas relacionadas con las redes personales	16
2.4.1. Redes móviles ad-hoc	16
2.4.2. Computación y comunicación ubicua	17
2.4.3. Wireless World Research Forum	18
2.4.4. Ambient Networks	19
2.4.5. PACWOMAN	19
2.4.6. SHAMAN	20
2.4.7. MobiLife	20
2.4.8. Entorno Personal Distribuido	21
2.4.9. MyNet	22
2.4.10. P2P Universal Computing Consortium	23

2.4.11. Otras iniciativas	23
2.5. Resumen	25
3 Hacia las redes personales	27
3.1. Concepto de red personal	28
3.1.1. Terminología	30
3.2. Visión general de la arquitectura de una PN	33
3.3. Capa de Abstracción a Nivel de Conectividad	36
3.4. Capa Universal de Convergencia	38
3.4.1. Principios de diseño	39
3.4.1.1. Abstracción del nivel de enlace	39
3.4.1.2. Entidad cognitiva	39
3.4.1.3. Independencia de los servicios	40
3.4.1.4. Proveedor de contexto	41
3.4.2. Descripción general	41
3.4.2.1. Capa de adaptación	41
3.4.2.2. Motor cognitivo de decisión	44
3.4.2.3. Descubrimiento de vecinos	46
3.4.2.4. Repositorio de información	47
3.4.2.5. Interfaz contextual	47
3.4.2.6. Adaptadores de protocolo	47
3.5. Capa de Abstracción a Nivel de Red	49
3.5.1. Formación de <i>clusters</i> y de la P-PAN	51
3.5.2. Formación de la PN	54
3.5.3. Direccionamiento en una PN	57
3.5.3.1. Formato	58
3.5.3.2. Asignación	60
3.5.4. Mantenimiento de la PN	61
3.5.5. Comunicaciones con nodos externos	63
3.5.6. Flujo interno entre componentes funcionales de los nodos	64
3.6. Capa de Abstracción a Nivel de Servicio	65
3.6.1. Conceptos previos	67
3.6.2. Descripción de alto nivel	68
3.6.3. Entorno de creación	69
3.6.4. Entorno de publicación y descubrimiento	70
3.6.5. Entorno de provisión y ejecución	73
3.6.6. Plataforma de usuario	75
3.6.7. Interacción entre componentes funcionales	75
3.6.7.1. Descubrimiento de servicios	76
3.6.7.2. Composición y ejecución de servicios	78
3.7. Capa de Abstracción a Nivel de Contexto	79
3.7.1. Descripción de alto nivel	82
3.7.1.1. Interfaz de acceso al contexto	83
3.7.1.2. Controlador del agente de contexto	84
3.7.1.3. Gestor de acceso al contexto	84
3.7.1.4. Módulo de comunicaciones	86

3.7.1.5.	Módulo de almacenamiento, razonamiento y procesamiento	86
3.7.1.6.	Gestor de seguridad	87
3.7.1.7.	Capa de abstracción de fuentes de datos de contexto	87
3.7.1.8.	Fuentes de datos	89
3.7.2.	Entidades funcionales	90
3.7.3.	Operativa general	91
3.7.4.	Modelado del contexto	93
3.7.5.	Lenguaje CALA	95
4	Seguridad y privacidad	99
4.1.	Terminología	100
4.2.	Notación	100
4.3.	Procedimiento de marcado	101
4.3.1.	Descripción del protocolo	103
4.3.2.	Gestión de claves	106
4.3.3.	Propiedad de transitividad	106
4.4.	Procedimiento de marcado certificado	107
4.4.1.	Inicialización y personalización mediante la PNCA	110
4.4.2.	Generación de las claves bilaterales compartidas a largo plazo	112
4.4.3.	Revocación de pertenencia a la PN	114
4.4.3.1.	Distribución de CRL jerarquizada	117
4.4.3.2.	Intercambio P2P de CRL	118
4.4.4.	Resiliencia de la PNCA	120
4.5.	Seguridad multicapa	121
4.5.1.	Seguridad a nivel de enlace	122
4.5.2.	Seguridad a nivel de red	126
4.5.3.	Seguridad a nivel de servicio	128
4.5.4.	Visión global	131
5	Federación de redes personales	133
5.1.	Concepto de federación	134
5.1.1.	Terminología	137
5.2.	Ciclo de vida	139
5.2.1.	Definición de perfiles	140
5.2.1.1.	Perfil de la PN-F	140
5.2.1.2.	Perfil de participación	142
5.2.2.	Participación en la PN-F	143
5.2.3.	Formación de la PN-F	144
5.2.4.	Uso de la PN-F	144
5.2.5.	Disolución de la PN-F	144
5.2.6.	Otra perspectiva del ciclo de vida	145
5.3.	Arquitectura	145
5.3.1.	Entidades funcionales comunes	149
5.3.1.1.	Directorio de redes personales	149
5.3.1.2.	Evaluador de políticas	151
5.3.1.3.	Asistente de federación	152

5.3.2.	PN-F sobre red virtual	153
5.3.2.1.	Publicación y descubrimiento	155
5.3.2.2.	Asociación	158
5.3.2.3.	Formación	160
5.3.2.4.	Utilización de los servicios	164
5.3.3.	PN-F empleando un intermediario de servicios	164
5.3.3.1.	Creación y asociación segura	166
5.3.3.2.	Participación y formación	167
5.3.3.3.	Utilización de los servicios	167
6	Validación experimental	171
6.1.	Certificación de la PNCA	174
6.1.1.	Arquitectura <i>software</i> del PNDS	175
6.1.2.	Procedimiento de certificación en MAGNET	176
6.1.3.	Procedimiento de certificación modificado	177
6.1.3.1.	Descripción funcional	178
6.1.3.2.	Estructura de datos	180
6.1.3.3.	Interfaz de gestión local	182
6.1.3.4.	Protocolo de intercambio remoto	182
6.2.	Capa Universal de Convergencia	190
6.2.1.	Arquitectura <i>software</i>	190
6.2.1.1.	Flujo de datos	196
6.2.2.	Análisis del retardo adicional	199
6.2.3.	Soporte multicanal radio	200
6.2.3.1.	Selección dinámica de la interfaz de salida	201
6.2.3.2.	Agregación de tráfico	204
6.3.	Protocolo de elección del gestor dentro de un <i>cluster</i>	207
6.3.1.	Función de coste	209
6.3.1.1.	Conectividad $C(v)$	209
6.3.1.2.	Recursos del nodo $R(v)$	210
6.3.2.	Descripción	211
6.3.3.	Adquisición de datos	215
6.3.3.1.	Recolector del sistema operativo	216
6.3.3.2.	Recolector de la UCL	217
6.3.4.	Evaluación	218
6.3.4.1.	Simulación	218
6.3.4.2.	Integración en SCMF y SMP	220
6.4.	Movilidad en la PN	221
6.4.1.	Arquitectura de la PN adaptada a MIPv6	222
6.4.2.	Plataforma de experimentación	223
6.4.2.1.	<i>Hardware</i> empleado	223
6.4.2.2.	Implementaciones MIPv6 en Linux	224
6.4.3.	Despliegue realizado	224
6.4.3.1.	Soporte MIPv6 a nivel de red	224
6.4.3.2.	Gestión del traspaso mediante NFC	227
6.4.3.3.	Interfaz de usuario	228

6.4.4. Evaluación de rendimiento	230
7 Conclusiones	235
7.1. Hacia la Internet del Futuro	239
Bibliografía	243
A Caracterización del canal inalámbrico IEEE 802.11	263
A.1. Análisis del escenario	263
A.2. Rendimiento de las interfaces radio	265
A.2.1. Tráfico UDP	267
A.2.2. Tráfico TCP	269
A.3. Herramientas de medida empleadas	271
B Publicaciones	273
B.1. Capítulos de libros	273
B.2. Revistas internacionales	273
B.3. Conferencias internacionales	274
B.4. Conferencias nacionales	276
B.5. Solicitudes de patentes	276
B.6. Ponencias y cursos	276
B.7. Documentos científico-técnicos	278
Thesis summary	287

Índice de figuras

1.1. Mapa de las tecnologías de comunicaciones inalámbricas	3
1.2. Relaciones entre los capítulos de la tesis	5
2.1. Modelo de referencia Multi-Esfera	18
2.2. Modelo de red según PDE	21
2.3. Pila de protocolos de la plataforma PUCC	23
3.1. Ejemplo de una red personal	29
3.2. Relaciones entre las principales entidades de una PN	33
3.3. Comparativa de modelos de red	34
3.4. Visión de una PN en capas de abstracción	35
3.5. Capa de Abstracción a Nivel de Conectividad	36
3.6. Ejemplo de nodo operando en múltiples dominios radio	38
3.7. Visión de planos de control y datos de la UCL	40
3.8. Arquitectura de alto nivel de la UCL	42
3.9. Interacciones en la Capa de Adaptación	43
3.10. Gestión multiradio en la UCL	44
3.11. Interacciones en el Motor Cognitivo de Decisión	45
3.12. Capa de Abstracción a Nivel de Red	49
3.13. Arquitectura de nivel de red de una PN	50
3.14. Proceso de formación de la P-PAN	53
3.15. Plataforma distribuida del agente de la PN	55
3.16. Evolución del procedimiento de conexión entre <i>clusters</i>	56
3.17. Formato de dirección personal	59
3.18. Diagrama de flujo de auto-configuración del prefijo de la PN	61
3.19. Gestión dinámica de los túneles y encaminamiento a nivel PN	62
3.20. Interfaces de interacción en un nodo personal	65
3.21. Capa de Abstracción a Nivel de Servicio	66
3.22. Arquitectura de la plataforma de gestión de servicios	68
3.23. Detalle de un componente de servicio	70
3.24. Paradigma de gestión de servicios multinivel	71
3.25. Red distribuida de intercambio entre SMN	72
3.26. Ejemplo de composición de servicios a partir de componentes	74
3.27. Gestión de la sesión de servicio	74
3.28. Secuencia del descubrimiento, composición y ejecución de servicios	76

3.29. Detalle de interacciones entre componentes para el descubrimiento y selección de un servicio	77
3.30. Detalle de interacciones entre componentes para la composición y ejecución de un servicio	79
3.31. Usos de la información de contexto	81
3.32. Visión global de la plataforma de gestión segura del contexto	82
3.33. Arquitectura de alto nivel de la SCMF	83
3.34. Arquitectura del CMI	84
3.35. Modos de intercambio de la información de contexto	85
3.36. Arquitectura del CAM	85
3.37. Arquitectura del P&S	86
3.38. Arquitectura de la DSAL	88
3.39. Representación de la DSAL con fuentes de datos distribuidas en los niveles OSI	89
3.40. Entidades funcionales de la SCMF	90
3.41. Etapas en la operativa de la SCMF	91
3.42. Interacciones en la SCMF a nivel de <i>cluster</i>	93
3.43. Interacciones en la SCMF a nivel de PN	93
3.44. Descripción de la entidad Nodo Personal (Personal Node)	95
3.45. Ejemplo de petición-respuesta en lenguaje CALA	96
4.1. Escenario de ejecución del protocolo de marcado	103
4.2. Protocolo de marcado	104
4.3. Propagación de la confianza mediante la propiedad de transitividad	107
4.4. Procedimiento de aplicación de la propiedad de transitividad	108
4.5. CPFPP empleando un PAC privado	111
4.6. CPFPP empleando un PAC público	112
4.7. Proceso de derivación de las claves bilaterales compartidas a largo plazo	113
4.8. CPFPP con intercambio de CRL	118
4.9. Protocolo de autenticación y securización del canal con intercambio de CRL	119
4.10. Jerarquía de derivación de claves en una PN	122
4.11. Proceso de derivación de claves en una PN	123
4.12. Derivación de claves de sesión a nivel de enlace	124
4.13. Formato de paquete cifrado y firmado entre nodos personales	125
4.14. Seguridad a nivel de enlace en un escenario multisalto	126
4.15. Provisión de servicio personal a un nodo personal	129
4.16. Provisión de servicio personal a un nodo externo	130
4.17. Visión global de la seguridad en una PN	131
5.1. Concepto de federación de redes personales	135
5.2. Relación entre roles dentro de una PN-F	137
5.3. Ciclo de vida de una PN-F	139
5.4. Perfiles dentro de la PN-F	140
5.5. Diagrama de estados de los participantes en la PN-F	146
5.6. Arquitectura y entidades funcionales de una PN-F	147
5.7. Arquitecturas de PN-F	148
5.8. Adaptación del proceso de iniciación de la PNCA	150

5.9. Arquitectura del PE	152
5.10. Máquina de estados simplificada del FM	153
5.11. Arquitectura del FM	153
5.12. PN-F como red virtual a nivel de red	154
5.13. PN-F sobre red virtual sustentada en infraestructura	155
5.14. PN-F ad-hoc sobre red virtual	155
5.15. Publicación y descubrimiento de PN-F en modo infraestructura	156
5.16. Publicación y descubrimiento de PN-F en modo ad-hoc	157
5.17. Proceso de autenticación y derivación de claves en PN-F ad-hoc	159
5.18. Descubrimiento de <i>clusters</i> en la PN-F	162
5.19. Uso PN-F en modo ad-hoc	164
5.20. PN-F empleando un intermediario de servicios	165
5.21. Flujo de información en una PN-F empleando un intermediario de servicios	166
5.22. Secuencia de ciclo de vida de PN-F basada en SP	169
6.1. Despliegue del entorno de evaluación de PN y PN-F en MAGNET	172
6.2. Diagrama de bloques de un nodo personal y su PN	173
6.3. Estructura <i>software</i> del PNDS	176
6.4. Interfaz de creación de cuenta sobre tableta	176
6.5. Proceso de certificación sobre tableta	177
6.6. Pantallas de inicio del proceso de firma	179
6.7. Protocolo de validación de identidad modificado	180
6.8. Formato del campo PIN	181
6.9. Pantalla de la interfaz de gestión del PIN	182
6.10. Estructura de los comandos y respuestas empleados para la autenticación	184
6.11. Estructura del comando “Envío de reto de autenticación”	184
6.12. Estructura del comando “Respuesta ante reto de autenticación”	185
6.13. Estructura del comando “Envío de confirmación de autenticación”	186
6.14. Estructura del comando “Cambio de clave”	187
6.15. Estructura de la respuesta “Cambio de clave”	188
6.16. Estructura del comando “Desbloqueo de clave”	189
6.17. Estructura de la respuesta “Desbloqueo de clave”	190
6.18. Arquitectura <i>software</i> de la UCL	191
6.19. Base de datos del módulo de descubrimiento de vecinos	193
6.20. Flujo de tráfico de salida a través de la UCL	198
6.21. Flujo de tráfico de entrada gestionado por la UCL	199
6.22. Escenario del experimento de selección dinámica de la interfaz de salida	201
6.23. Rendimiento del procedimiento de selección dinámica de la interfaz de salida	202
6.24. Rendimiento empleando únicamente la interfaz IEEE 802.11a	203
6.25. Rendimiento empleando únicamente la interfaz IEEE 802.11b	203
6.26. Agregación de tráfico empleando múltiples enlaces de comunicación	205
6.27. Agregación de tráfico empleando múltiples enlaces de comunicación	206
6.28. Escenario de validación experimental de la solución de agregación de tráfico	207
6.29. Rendimiento del procedimiento de agregación de tráfico	208
6.30. Proceso de selección y mantenimiento de gestor	212
6.31. Escenario de validación del proceso de selección del gestor	213

6.32. Formato de mensajes desafío-respuesta para el proceso de selección del gestor .	214
6.33. Detalle de la implementación del recolector de datos de batería	215
6.34. Entidades asociadas al sistema operativo	217
6.35. Entidades asociadas a la estructura de red	218
6.36. Evaluación del proceso de selección de gestor	219
6.37. Arquitectura de MIPv6 sobre MAGNET	222
6.38. Configuración global de red del entorno de pruebas MIPv6	226
6.39. Visión de los canales de comunicación del entorno de pruebas sin MIPv6	226
6.40. Canales de comunicación del entorno de pruebas con MIPv6 habilitado usando un equipo portátil	227
6.41. Canales de comunicación del entorno de pruebas con MIPv6 habilitado usando un cliente móvil	228
6.42. Formato de la información en la etiqueta NFC	228
6.43. Interfaz de usuario en teléfono móvil	229
6.44. Imagen del entorno de pruebas	230
6.45. Evolución del traspaso	231
7.1. Arquitectura de la Internet del Futuro	240
A.1. Escenario de la campaña de medidas	264
A.2. Caracterización del canal en función de la SNR	265
A.3. Función de distribución de probabilidad de la SNR	266
A.4. Evolución del rendimiento de las interfaces IEEE 802.11 en UDP según la loca- lización	268
A.5. Evolución del rendimiento de las interfaces IEEE 802.11 en TCP según la loca- lización	270

Índice de tablas

2.1.	Ejemplos de ataques según el nivel de la pila de protocolos	12
2.2.	Comparativa de iniciativas relacionadas con las redes personales	25
3.1.	Terminología vinculada a las redes personales	31
3.1.	Terminología vinculada a las redes personales (continuación)	32
3.1.	Terminología vinculada a las redes personales (continuación)	33
4.1.	Terminología de seguridad	100
4.2.	Nomenclatura empleada en seguridad	101
5.1.	Terminología vinculada a la federación de redes personales	137
5.1.	Terminología vinculada a la federación de redes personales (continuación) . . .	138
6.1.	Estructura de datos de la aplicación de autenticación	181
6.2.	Comparativa de rendimiento ofrecido por la UCL	200
6.3.	Estadísticas de rendimiento del procedimiento de selección dinámica de la interfaz de salida	201
6.4.	Estadísticas de rendimiento del procedimiento de agregación de tráfico	207
6.5.	Valores relativos asignados a los recursos	211
6.6.	Rendimiento del traspaso MIPv6	232
A.1.	Estadísticas de rendimiento de las interfaces IEEE 802.11 en UDP según la localización	267
A.2.	Estadísticas de rendimiento de los interfaces IEEE 802.11 en TCP según la localización	269

Índice de cuadros de texto

3.1. Ejemplo de codificación de una petición en lenguaje CALA	97
6.1. Registro de eventos SAT	178
6.2. Cambio de PIN	183
6.3. Creación del dispositivo virtual - Código de UCLk	194
6.4. Envío de paquetes - Código de UCLk	195
6.5. Interfaces I/O basadas en <i>Netlink sockets</i> - Código de UCLk	197
6.6. Interfaces I/O basadas en <i>Netlink sockets</i> - Código de UCLk (cont.)	198
6.7. Opciones de configuración del <i>kernel</i> de Linux para soportar MIPv6	225

Lista de acrónimos

3DES	Triple Data Encryption Standard
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting (Autenticación, autorización y compensación)
AC	Aplicador de Contexto
AdP	Adaptador de Protocolo
AdS	Agente de Servicio
AES	Advanced Encryption Standard
AH	Authentication Header
AI	Ambient Intelligence (Inteligencia ambiental)
AN	Ambient Networks
AODV	Ad hoc On Demand Distance Vector
APDU	Application Protocol Data Unit
API	Application Programming Interface
ARP	Address Resolution Protocol
ARR	Adaptador de Recursos Radio
BAN	Body Area Network (Red de área corporal)
BCN	Basic Context Node (Nodo básico de contexto)
BNEP	Bluetooth Networking Encapsulation Protocol
BSS	Basic Service Set
CA	Certification Authority (Autoridad de certificación)
CAC	Context Agent Controller (Controlador del agente de contexto)
CACo	Context Aware Component (Componente sensible al contexto)
CALA	Context Access LAnguage (Lenguaje de acceso al contexto)
CAM	Context Access Manager (Gestor de acceso al contexto)
CAN	Community Area Network (Red de área comunitaria)
CAS	Capa de Adaptación de Servicio
CASM	Context Aware Security Manager (Gestor de seguridad en el contexto)
CBC	Cyclic Block Ciphering
CdA	Capa de Adaptación
CENIT	Consortios Estratégicos Nacionales de Investigación Técnica
CMCa	Clave Maestra del Canal
CMCo	Clave Maestra de Comunicaciones

CMG	Context Management Gateway
CMI	Context Management Interface (Interfaz de acceso al contexto)
CMN	Context Management Node (Nodo gestor de contexto)
CN	Correspondent Node (Nodo corresponsal)
CNW	Context Node Weight (Peso asignado al nodo de contexto)
CoA	Care-of Address
CPFP	Certified PN Formation Protocol (Protocolo certificado de formación de la PN)
CQI	Channel Quality Indicator
CR	Coordinador Radio
CRC	Cyclic Redundancy Check (Código de redundancia cíclica)
CRL	Certificate Revocation List (Lista de certificados revocados)
CS	Compositor de Servicios
CSAIL	Computer Science and Artificial Intelligence Laboratory
CUP	Consensus with Unknown Participants (Consenso con participantes desconocidos)
DAD	Duplicate Address Detection (Detección de direcciones duplicadas)
D-Bus	Desktop Bus
DCCP	Datagram Congestion Control Protocol
DES	Data Encryption Standard
DH	Diffie-Hellman
DICOM	Departamento de Ingeniería de Comunicaciones
DLC	Data Link Control (Control de enlace de datos)
DME	Device Management Entity (Entidad gestora de dispositivos)
DoS	Denial of Service (Denegación de servicio)
DR	Dominio Radio
DSAL	Data Source Abstraction Layer (Capa de abstracción de fuentes de datos de contexto)
DSAM	Data Source Abstraction Manager (Gestor de fuentes de datos)
DTLS	Datagram Transport Layer Security
DYMO	Dynamic MANET On-demand Routing
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography (Criptografía basada en curvas elípticas)
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECMQV	Elliptic Curve MQV
ECN	Enhanced Context Node (Nodo avanzado de contexto)
EDR	Emulador de Dominio Radio
EESSI	European Electronic Signature Standardisation Initiative
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
ETSIIT	Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación
ETX	Expected Transmission Count Metric

FER	Frame Error Rate (Tasa de error de trama)
FHMQV	Fully Hashed MQV
FI	Future Internet (Internet del Futuro)
FM	Federation Manager (Asistente de federación)
FTP	File Transfer Protocol (Protocolo de transferencia de ficheros)
GAR	Gestor de Adaptadores de Recursos
GIAAC	Gestor de Identidad, Autenticación, Autorización y Compensación
GIS	Geographic Information System (Sistema de información geográfica)
GLL	Generic Link Layer
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRR	Gestor de Recursos Radio
GS	Gestor de Servicios
GSM	Global System for Mobile communications
HA	Home Agent (Agente local)
HAL	Hardware Abstraction Layer (Capa de abstracción de <i>hardware</i>)
HDR	High Data Rate (De alta velocidad de transmisión de datos)
HMAC	keyed-Hash Message Authentication Code
HMQV	Hashed MQV
HoA	Home Address
HP	Hewlett-Packard
HSDPA	High-Speed Downlink Packet Access
HTTP	Hypertext Transfer Protocol
I/O	Input/Output (Entrada/Salida)
IBBT	Interdisciplinary Institute for Broadband Technology
IBSS	Independent BSS
ICCID	Integrated Circuit Card Identifier (Identificador del chip de la tarjeta)
IDE	Integrated Device Electronics
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange
INT	Institut National des Télécommunications
IoK	Internet of Knowledge (Internet de los Contenidos y el Conocimiento)
IoS	Internet of Services (Internet de los Servicios)
IoT	Internet of Things (Internet de las Cosas)
IoU	Internet of Users (Internet de las Personas)
IP	Internet Protocol
IPC	Inter-Process Communication (Comunicación entre procesos)
IPSec	IP Secure
IrDA	Infrared Data Association (Asociación de datos infrarrojos)
ISO	International Organization for Standardization
IST	Information Society Technologies
ITU	International Telecommunication Union

LDR	Low Data Rate (De baja velocidad de transmisión de datos)
LV	Longitud Valor
MAC	Medium Access Control
MADM	Multi-Attribute Decision Making
MAGNET	My personal Adaptative Global NET
MANET	Mobile Ad hoc NETworks Working Group
MCD	Motor Cognitivo de Decisión
MCdS	Módulo de Calidad de Servicio
MIME	Multipurpose Internet Mail Extensions
MIP	Mobile IP
MIPL2	Mobile IPv6 for Linux v2.0
MIT	Massachusetts Institute of Technology
MN	Mobile Node (Nodo móvil)
MOPED	MObile grouPEd Device
MPD	Motor de Publicación y Descubrimiento
MQV	Menezes-Qu-Vanstone
MTM	Medium Time Metric
MTU	Maximum Transmission Unit (Unidad máxima de transmisión)
NAD	Network Address Device (Intermediario de acceso a red)
NAT	Network Address Translation (Traducción de direcciones de red)
ND	Neighbour Discovery
NDEF	NFC Data Exchange Format
NEMO	Network Mobility
NetCoM	Network Communication Module (Módulo de comunicaciones)
NFC	Near Field Communication (Comunicaciones de campo cercano)
NIST	National Institute of Standards and Technology
NS-2	Network Simulator v2
NW	Node Weight (Peso asignado a un nodo)
OAuth	Open Authentication
OLSR	Optimized Link State Routing Protocol
OMA	Open Mobile Alliance
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTA	Over-the-Air
OWL	Ontology Web Language
P2P	Peer-to-Peer (Entre iguales)
P&S	Processing and Storage (Módulo de almacenamiento, razonamiento y procesamiento)
PAC	Proximity Authenticated Channel (Canal autenticado en proximidad)
PACWOMAN	Power Aware Communications for Wireless Optimised Personal Area Network
PAN	Personal Area Network (Red de área personal)

PCOL	PAN and CAN Optimisation Layer
PDA	Personal Digital Assistant
PDE	Personal Distributed Environment (Entorno personal distribuido)
PDIF	Presence Information Data Format
PE	Policy Engine (Evaluador de políticas)
PEP	Performance Enhancing Proxy
PFP	PN Formation Protocol (Protocolo de formación de la PN)
PIN	Personal Identification Number (Número de identificación personal)
PKI	Public Key Infrastructure (Infraestructura de clave pública)
PMH	Personal Mobile Hub (Núcleo móvil personal)
PMP	Proactive MANET Protocol (Protocolo proactivo MANET)
PN	Personal Network (Red personal)
PNCA	Personal Network Certification Authority (Autoridad de certificación de la PN)
PNDS	Personal Network Directory Server (Directorio de redes personales)
PN-F	Personal Networks Federation (Federación de redes personales)
PNP 2008	Personal Networking Pilot 2008
P-PAN	Private Personal Area Network (Red privada del entorno de usuario)
PPP	Point-to-Point Protocol (Protocolo punto a punto)
PUCC	P2P Universal Computing Consortium
QoE	Quality of Experience (Calidad de experiencia)
QoS	Quality of Service (Calidad de servicio)
QR	Quick Response
RAM	Random Access Memory
RAT	Radio Access Technology (Tecnología de acceso radio)
RFID	Radio Frequency IDentification (Identificación por radio frecuencia)
RFU	Reserved for Future Use
RMP	Reactive MANET Protocol (Protocolo reactivo MANET)
RPC	Remote Procedure Call
RRP	Return Routability Procedure
RSSI	Received Signal Strength Indication
SAN	Service Assistance Node (Nodo asistente en la gestión de servicios)
SAT	SIM Application Toolkit
SCMF	Secure Context Management Framework (Plataforma de gestión segura del contexto)
SHA	Secure Hash Algorithm
SHAMAN	Secure Heterogeneous Access to Mobile Applications and Networks
SIM	Subscriber Identity Module
SLP	Service Location Protocol
SMN	Service Management Node (Nodo gestor de servicios)
SMP	Service Management Platform (Plataforma de gestión de servicios)
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol

SNR	Signal-to-Noise Ratio (Relación señal a ruido)
SOAP	Simple Object Access Protocol
SP	Service Proxy (Intermediario de servicios)
SPI	Security Parameters Indication
SSID	Service Set IDentifier
SSL	Secure Sockets Layer
SSO	Single Sign On
SW	Status Word (Bytes de estado)
TAR	Toolkit Application Reference
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLS-PSK	Transport Layer Security Pre-Shared Key
TOTP	Time-based One Time Password (Contraseña de un solo uso basadas en tiempo)
TTP	Trusted Third Party (Tercera entidad de confianza)
UC	Universidad de Cantabria
UCL	Universal Convergence Layer (Capa universal de convergencia)
UDP	User Datagram Protocol
UE	Unión Europea
UGI	User Generated Identifier (Identificador generado por el usuario)
UIA	User Information Architecture
UIP	Unmanaged Internet Protocol
UMIP	Universal MIP
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications System
UPN	Universal Personal Networking
UPnP	Universal Plug and Play
USAGI	UniverSAl playGround for Ipv6
USB	Universal Serial Bus
UWB	Ultra Wide Band
VCE	Virtual Centre of Excellence
VoIP	Voice over IP (Voz sobre IP)
VPN	Virtual Private Network (Red privada virtual)
VTT	Valtion Teknillinen Tutkimuskeskus
WAL	Wireless Adaptation Layer
WAN	Wide Area Network (Red de área extensa)
WCETT	Weighted Cumulative Expected Transmission Time
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WINE	Wireless Internet NEtworks
WLAN	Wireless Local Area Network (Red de área local inalámbrica)
WPA	Wi-Fi Protected Access

WPAN	Wireless Personal Area Network (Red de área personal inalámbrica)
WWI	Wireless World Initiative
WWRF	Wireless World Research Forum
XML	eXtensible Markup Language

Capítulo 1

Introducción

La capacidad de transformación y adaptación al entorno ha marcado la evolución del ser humano y la ambición, como característica innata, le ha conducido a sobrepasar sus límites en aras de conseguir unas metas autoimpuestas. Aunque sin ser un rasgo diferencial de la especie humana, la comunicación ha jugado un papel protagonista en su desarrollo.

La historia de la comunicación tiene su origen millones de años atrás; el hombre, siempre ha buscado una forma de compartir sus pensamientos y acciones. El desarrollo del lenguaje trajo consigo una ventaja evolutiva que se supo aprovechar para comunicar de manera eficiente información de generación en generación, promover la compartición de conocimiento o coordinarse de manera eficiente para la realización de tareas. El paso de los años conllevó la consolidación progresiva del uso del lenguaje, presentándose entonces el reto de definir nuevas formas más eficientes de comunicación.

La distancia y el tiempo han sido las serias y evidentes limitaciones de cualquier modelo de comunicación. El disponer de un canal de comunicaciones simétrico donde todas las partes involucradas puedan participar activamente en el intercambio de información es otra más. Sin embargo el hombre siempre se las ha ingeniado para solucionar cualquier situación y es ahí donde la tecnología ha entrado para facilitar las cosas.

El lenguaje oral evolucionó hacia la escritura con el objeto de conservar el conocimiento. Restringida a los estratos sociales más poderosos durante la mayor parte de la historia antigua, la imprenta permitió el acceso a la cultura a casi cualquier persona, momento a partir del cual la evolución sufrió una gran impulso.

Sin embargo no es hasta mediados del siglo XIX, de la mano Samuel Morse con la invención del primer telégrafo, que se produce otra gran revolución de las comunicaciones: lograr transmitir de manera casi instantánea un mensaje entre dos puntos separados geográficamente. A partir de aquí, la aparición del teléfono o la radio no hicieron sino mejorar la forma en la que la información se intercambia.

Cuando la capacidad intelectual para desarrollar nuevas opciones se vio limitada, el nacimiento de los primeros ordenadores al final de la primera mitad del siglo pasado, provoca un nuevo empuje a nivel evolutivo, cuya aceleración aún hoy en día sigue en aumento.

La búsqueda de la convergencia entre el mundo de la computación y de la comunicación llevó durante la década de los sesenta a idear Internet como una red que permitiera com-

partir información entre nodos autónomos, distribuidos y organizados en múltiples redes independientes en diferentes localizaciones. Un concepto clave de Internet es que no se había diseñado para dar soporte a una única aplicación, sino como una infraestructura genérica en la que se podían desplegar nuevas y múltiples aplicaciones. Esa característica es la que ha supuesto que la creación de un pequeño grupo de investigadores se pueda considerar la última gran revolución en la forma de comunicar conocimiento.

Internet se concibió como una red de arquitectura abierta para compartir recursos en lugar de replicarlos. La selección de la tecnología de acceso no estaba explicitada, sino que la podía elegir libremente un proveedor y hacerla interactuar con las restantes redes. Esta filosofía pronto hizo que el acceso a todos esos recursos se habilitara a través de redes de paquetes por satélite, redes móviles, redes inalámbricas y otras, en las que la conexión mediante cables quedaba relegada a un segundo plano usualmente como parte de la red troncal.

Esta tendencia se desencadenó como resultado de la demanda de los usuarios por entornos más flexibles que les dotaran de las capacidades de acceso en movilidad. De esta forma, los recursos estarían a su alcance en cualquier momento y lugar, logrando la tan ansiada ubicuidad. Se había encontrado la manera de superar las barreras que la distancia y el tiempo imponían a la comunicación.

Esta necesidad se planteó inicialmente en el mundo empresarial, donde inicialmente el principal requerimiento era el acceso a servicios provistos por redes de área extensa (WAN, *Wide Area Network*). Con la eclosión de las tecnologías de comunicaciones móviles terrestres e inalámbricas a finales del milenio pasado, poco a poco este modelo de acceso a la información se fue haciendo más popular. En este nuevo entorno los requerimientos cambiaron. El usuario general lleva la demanda del servicio hacia él, migrando el uso de servicios WAN a servicios más cercanos disponibles a través de red de área local inalámbrica (WLAN, *Wireless Local Area Network*).

Aunque deseado por muchos, los costes del equipamiento necesario provocaron que la velocidad de penetración no fuera elevada en los inicios. No obstante, el continuo avance en la integración de la tecnología microelectrónica ha permitido no solo un notable incremento en las capacidades de cómputo, sino que ha posibilitado la integración de un mayor número de funcionalidades en los dispositivos, entre ellas de comunicaciones, al tiempo que ha abaratado los costes de producción y venta.

Al tiempo que la tecnología se ha hecho más asequible y portátil, la sociedad ha reclamado la adaptación de los servicios al ámbito más próximo a ellos, lo que ha desembocado en el desarrollo y despliegue de un nuevo abanico de tecnologías de transmisión englobadas dentro de los que se ha dado en llamar redes de área personal inalámbricas (WPAN, *Wireless Personal Area Network*). Estas tecnologías permiten la conexión de portátiles, teléfonos móviles o cualquier otro dispositivo personal en un entorno de hasta 10 metros de forma transparente a alta velocidad y con un bajo consumo energético.

La gran variedad de medios por los que acceder a los recursos, ha hecho que en los últimos años, los usuarios de Internet hayan crecido de forma exponencial, pudiéndose considerarse el acceso a la información es ahora mismo universal. Ya lo predijo Bill Gates hace 20 años: «toda la información que necesitamos y más, está literalmente en la punta de nuestros

dedos y cabe en los bolsillos de nuestros abrigos» [1]. Sin embargo, aunque la información, servicios, aplicaciones y cualquier recurso esté accesible a través de casi cualquier dispositivo, la mayoría de los usuarios no sabe gestionar esa diversidad de forma inteligente y desborda sus expectativas y, lo que es más, sus capacidades.

Si se hace un mapa de las tecnologías de comunicaciones inalámbricas disponibles en la actualidad, como el mostrado en la figura 1.1, se observa la existencia de un gran cúmulo de ellas producto de la adecuación de cada una a un área muy específico en cuanto a tasa binaria, cobertura, modo de uso, etc. Además, la interoperabilidad entre la mayoría no es posible.

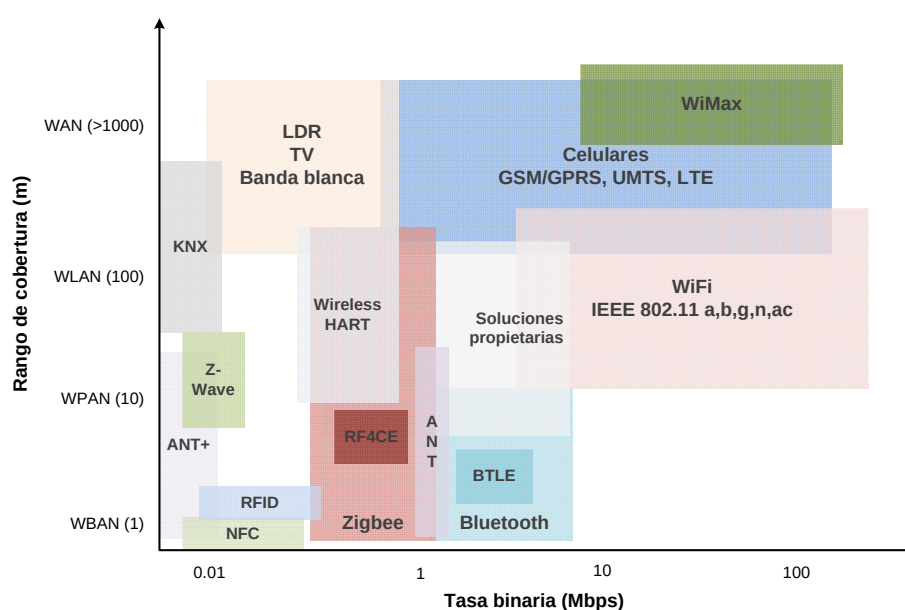


Figura 1.1: Mapa de las tecnologías de comunicaciones inalámbricas

La misma labor se podría hacer para los modelos y arquitecturas de dispositivos de acceso y servicios, obteniendo un resultado muy similar. Esto se traduce en dificultades para los usuarios que tienen que aceptar esta diversidad y adquirir el conocimiento suficiente en cada una de ellas para su uso.

Desafortunadamente, poco esfuerzo se ha hecho por integrar todas las tecnologías y dar al usuario la importancia que se merece, ofreciéndole una experiencia de uso única, independiente y adaptada a sus necesidades y preferencias. Si bien es cierto que en el ámbito de la investigación algunas tentativas se han realizado, a nivel comercial no se han observado soluciones globales. El mayor logro hasta el momento es que cada empresa en particular, como son los ejemplos de Apple, Google o Microsoft, integre los servicios, aplicaciones y dispositivos propios de su ecosistema. Pero ésta no es la respuesta que se desea y espera.

1.1. Motivación y objetivos

Dentro del marco descrito, se identifican diversas carencias. La mayoría de ellas apuntan en una dirección, el usuario. Aunque la evolución tecnológica ha sido dirigida por él, también

es él quien guía a los instrumentos, que ha diseñado y desarrollado, para que realicen las tareas que se requieren. El ser humano se ha olvidado de que él mismo es juez y parte y que debería de haber dotado de autonomía al ecosistema creado para que no sólo actúe a sus órdenes, sino que inteligentemente reaccione ante los cambios en sus necesidades y preferencias.

En este sentido, tal como se puede inferir de la descripción anterior, el creciente número de dispositivos de usuario, ya no solo en su entorno más cercano, sino también aquellos que se encuentran en su hogar, oficina, etc., interaccionan entre sí, definiendo una red cuyas características dejan de ser genéricas. Esta red, a la que se puede denominar personal, tiene un claro enfoque en el usuario. Deberá ser una red inteligente y más sensible al contexto, lo que provocará que el comportamiento de los nodos y servicios que la conforman se acomoden a los requerimientos de su propietario. Por tanto, la experiencia de uso de dos usuarios con un equipamiento similar podrá ser totalmente diferente puesto que las correspondientes redes los conocerán y se adaptarán a ellos.

El concepto de red personal (PN, *Personal Network*) expande el de la tradicional red de área personal (PAN, *Personal Area Network*) en tanto en cuanto abarca dispositivos y servicios remotos fuera del alcance físico del usuario. Será la propia PN la que acercará al usuario cualquiera de sus terminales habilitando un acceso ubicuo y transparente a través de las redes subyacentes. Las implicaciones del despliegue de una PN van más allá de la provisión de conectividad entre sus nodos, debiendo garantizar la interoperabilidad con otras redes, como la propia Internet, en las que reside un gran volumen de servicios de valor añadido a disponibilidad del usuario.

Por tanto, la ubicuidad y el contexto son dos aspectos claves iniciales que dan sentido a la PN. La seguridad será el tercero, que hará que el usuario confíe en que su privacidad se protege en todo momento y los datos de los servicios que consuma o provea a otros usuarios no se verán comprometidos.

Responder a cuestiones como cómo lograr una experiencia de comunicación ubicua mediante tecnologías heterogéneas, qué mecanismos emplear para desarrollar, consumir y proveer servicios sobre esa red, cómo adaptar la respuesta de la red al contexto y, sobre todo, cómo facilitar la configuración y uso de una red tan ambiciosa, articularán los desarrollos llevados a cabo y permitirá dotar a la PN de unos pilares sólidos y estables.

1.2. Estructura de la tesis

El presente trabajo tiene como objetivo global definir una arquitectura que dé soporte a una red personal, como extensión de una PAN, y a las agrupaciones de ellas. Para ello más allá de concebir diferentes propuestas de diseño, aborda la evaluación experimental de aquéllas, de forma que se pueda validar su viabilidad.

La metodología empleada se representa en la figura 1.2. Así, en el capítulo 2 “Requerimientos e iniciativas relacionadas” se analizan un conjunto de casos de uso canónicos de los que se extraen los correspondientes requerimientos tanto para las redes personales como para la federación de ellas. Seguidamente se presenta un somero estado del arte en cuanto a iniciativas previas relacionados de un modo u otro con algunos de los conceptos citados.

PN-F y su ciclo de vida desde su creación hasta su disolución, considerando las condiciones que una PN debe cumplir para pasar a formar parte de una PN-F y cuáles son los mecanismos para garantizar la confianza y seguridad dentro de la PN-F. En el citado capítulo se plantea una arquitectura genérica, la cual se particulariza según dos aproximaciones: la PN-F planteada como una agregación sustentada a nivel de red y sobre la que se comparten todo tipo de recursos (conexión, servicios, etc.) o la PN-F considerada únicamente a nivel de servicio.

El capítulo 6 “Validación experimental” aborda la validación experimental de las propuestas realizadas por este autor en el marco de los proyectos *Information Society Technologies* (IST) *My personal Adaptative Global NET* (MAGNET) y MAGNET Beyond, así como otras llevadas a cabo en el marco de colaboraciones adicionales.

Para finalizar, en el capítulo 7 “Conclusiones” se recogen las principales aportaciones realizadas y se establece una propuesta de líneas de investigación que emanan de la investigación desarrollada en esta tesis.

Capítulo 2

Requerimientos e iniciativas relacionadas

Antes de desarrollar los conceptos de PN y de PN-F como una agrupación de PN, es importante identificar y comprender cuáles son los aspectos que hay que resolver. Es por esto que en este capítulo se realiza un análisis de las características de ambos modelos y se identifican los requerimientos de alto nivel de cada uno.

Para ello se emplean una serie de casos de uso que permiten visualizar la PN y la PN-F en escenarios reales y así entender mejor las necesidades y su relevancia. Los casos de uso descritos se deben tomar como ejemplos. Las PN se podrán aplicar en otro gran número de situaciones que nada tienen que ver con las detalladas aquí.

Por último, y antes de abordar los trabajos de diseño, especificación e implementación, se realiza un breve análisis de iniciativas que en el momento de iniciar el desarrollo de esta tesis podrían ayudar en la consecución de los objetivos planteados para las PN. Será sobre las carencias que se detecten sobre las que posteriormente se hará más hincapié.

2.1. Escenarios y casos de uso

A continuación se describen diversos casos de uso como ejemplo de situaciones reales donde se muestra la operativa prevista tanto para las PN como para las PN-F.

2.1.1. Cuidado remoto de niños

Una pareja de padres acude a una cena entre amigos. Puesto que es la primera vez que dejan a su recién nacido a cargo de otra persona, tienen el temor de que algo le pueda pasar, a pesar de que es la abuela quien se ha quedado con él. Como regalo por el nacimiento, los amigos les han obsequiado con un sistema de vigilancia formado por una cámara con micrófono que puede conectarse a la red del hogar. Habilitando el acceso remoto pueden observar al niño en cualquier lugar.

Los padres disponen de teléfonos inteligentes de última generación en los que han instalado la aplicación necesaria para acceder de manera segura y autenticada al sistema de vigilancia.

Al llegar a casa de sus amigos, la madre se conecta empleando su terminal móvil a la red del hogar y accede a las imágenes que está transmitiendo la cámara. Para tener mejor calidad de imagen, selecciona la opción de iluminar levemente la habitación.

Los amigos, ansiosos por ver al bebé, le solicitan que les preste su teléfono. En lugar de ello, prefiere compartir la imagen empleando la pantalla de televisión de sus amigos, una vez que ellos le han cedido el acceso tanto a la pantalla como a la red de su hogar.

2.1.2. Ejecutiva del mercado de valores

Laura se prepara para un nuevo día de trabajo y enciende su dispositivo móvil equipado con las últimas tecnologías de comunicaciones.

Laura necesita ver las noticias de la bolsa del canal de negocios, debido a que espera importantes noticias que se anunciarán durante el día y que pueden afectar a las inversiones que tiene realizadas. Para ello ejecuta una aplicación de vídeo que la permite ver la emisión de dicho canal. Laura ha configurado ese canal para que se vea siempre con la mejor calidad posible. Cuando inicia el vídeo sólo tiene acceso a la red móvil de su proveedor, por lo que el vídeo se descarga con una calidad aceptable empleando la interfaz de comunicaciones adecuada.

Cuando Laura entra en su empresa, su terminal detecta el nuevo emplazamiento y comienza la búsqueda de redes *Wireless Fidelity* (WiFi) en su entorno. Ella tiene prefijado el uso de esa nueva tecnología de comunicación para reducir los gastos en que repercutiría el uso de la red celular. Cuando finalmente llega a su despacho, el vídeo, recibido a través de la red WiFi de la empresa, pasa a ser mostrado en la pantalla de su ordenador.

Durante todo el trayecto entre su casa y su despacho la calidad de la emisión no se ha visto degradada notablemente, ni se ha interrumpido.

2.1.3. Viaje de trabajo

Dos compañeros de trabajo se están desplazando a una importante reunión en la que tienen que presentar el nuevo producto desarrollado por su empresa. Han preferido ir en tren dado que aún no tienen totalmente finalizada la presentación y este medio de transporte les ofrece mejores opciones para continuar el trabajo.

Cada uno pone a disposición del otro los recursos compartidos de su portátil y teléfono móvil, creando una versión reducida de su oficina. Por tanto, tendrán acceso a todos los ficheros, documentos, imágenes, etc. Colaborativamente continúan editando la presentación, intercambiando opiniones sobre las modificaciones que están llevando a cabo.

Cuando tienen la versión definitiva de la presentación, deciden compartirla con su jefe, que no ha podido desplazarse con ellos y se encuentra en la oficina. Inician con él una videoconferencia en la que discuten el nuevo contenido. La conexión que tienen disponible en el tren no ofrece la suficiente calidad, así que deciden emplear conjuntamente los canales de comunicación de los teléfonos móviles para tener un mayor ancho de banda, pero empleando únicamente uno de ellos para la visualización. De esta forma obtienen una mejor calidad de imagen y sonido.

Cuando la batería del terminal empleado para seguir la videoconferencia está en un nivel muy bajo, automáticamente se realiza el traspaso a la pantalla del otro, que tiene más batería remanente.

Durante la reunión su jefe les da la enhorabuena por el buen trabajo y les desea suerte en la presentación al potencial cliente.

2.1.4. Vendedor ambulante

Un vendedor está realizando las visitas a las tiendas que se encuentran en su ruta asignada. Al entrar en un comercio se presenta al encargado del establecimiento e intercambia digitalmente su tarjeta de visita. Esta acción evita posibles errores en el momento que el cliente pretenda comunicarse con él pues sus datos de contacto, con el consentimiento de ambos, se incorporan directamente a su agenda.

Para realizar la demostración del producto, tal como habían acordado, el establecimiento le proporciona un acceso a su red de invitados (la red privada no estará accesible) y a los equipos de la pequeña sala de reuniones.

Los dispositivos del vendedor al entrar en el establecimiento han detectado la nueva localización, han localizado las credenciales de acceso asociadas y han transferido los catálogos y presentaciones al equipo de la sala. Tras realizar la presentación, el encargado se muestra satisfecho con los productos y decide mantener una colaboración con la empresa del vendedor. Para mantenerse informado de posibles cambios en el catálogo y de cualquier otra noticia, decide extender el acuerdo previo durante un período ilimitado, lo que permitirá al vendedor actualizar el contenido del catálogo de forma remota y notificarlo.

Al salir de la tienda, el vendedor se encuentra con un amigo que ha empezado a trabajar en una empresa cuyos productos son compatibles con los que él provee y que podrían venderse de forma conjunta, ampliando así ambos la cartera de clientes. En lugar de intercambiarse los catálogos y fichas técnicas, deciden configurar sus equipos para que automáticamente se pongan en contacto ante actualizaciones.

2.2. Requerimientos de una red personal

Como ha quedado patente en los casos de uso anteriores, en las PN, el usuario es el elemento central y la red se genera para dar respuesta a sus necesidades de acceso a servicios. En este sentido, antes de proceder a definir soluciones hay que conocer los requerimientos y preferencias de los potenciales usuarios y del entorno en el que se mueven.

De forma general se pueden definir dos perfiles de usuarios: privado u ordinario y profesional. Ambos se segmentan aún más en función de sus áreas de actuación, edad, etc. presentando una mayor diferenciación. No obstante, en lugar de afinar esta división, es más importante señalar que en muchos casos el rol de un usuario varía o incluso las necesidades de cada perfil se solapan.

Para el perfil del usuario profesional, las redes son una herramienta para llevar a cabo las tareas relacionadas con su actividad laboral, donde se valora la productividad sobre el coste. En este entorno además, la estabilidad de los servicios, la adaptación de los mismos

y de las redes de acceso y, sobre todo, la seguridad en los intercambios tienen una gran importancia.

Por su parte, el usuario cotidiano emplea las redes para facilitar las tareas de su vida cotidiana y mejorar su calidad de vida. Esta característica se solapa con las previstas para el usuario profesional. Sin embargo, el coste de los servicios, en la mayoría de los casos se prioriza sobre la calidad de servicio (QoS, *Quality of Service*) y la calidad de experiencia (QoE, *Quality of Experience*). Otra diferencia entre ambos perfiles es la diversidad de usos, lo que hace que el abanico de requerimientos sea virtualmente infinito [2].

Otra clasificación muy común que se realiza del usuario emana de su papel ante un recurso, ya sea, por ejemplo, un servicio o el acceso a la red. En ese caso, se diferencia entre el usuario consumidor o proveedor. Desde el punto de vista de operativa de los servicios y de la propia red y, más aun, de seguridad, presentan retos muy interesantes a la hora de afrontar el diseño de una PN y, especialmente, del modelo de colaboración entre ellas.

Seguidamente se presentan un conjunto de requerimientos para las PN, que independiente del perfil del usuario, permitan más adelante diseñar soluciones globales para ellas. De la misma forma, estos requerimientos servirán para validar la especificación y despliegue de estas redes. Cabe señalar que los requerimientos básicos de las PN-F se extienden de los identificados para las PN, pues al fin y al cabo la nueva red se forma a partir de las PN con un objetivo conjunto, servir a todos los usuarios. Por tanto, no se hará falta especial hincapié en ellos, a excepción de los vinculados con la seguridad, las políticas de acceso y la definición y la publicación de las preferencias, pues son específicos de las PN-F.

Los requerimientos se agrupan en cinco categorías y si bien éstos se describen con un cierto grado de abstracción, es importante reseñar que se ha buscado formularlos de modo que permitan identificar las problemáticas a resolver y guiar las posibles líneas de investigación y desarrollo que de ellos surjan.

2.2.1. Facilidad de uso

Lo primero que evalúa un usuario es aquello que tiene más accesible y realiza con más frecuencia. Por lo tanto, uno de los más importantes requerimientos que la especificación de las PN debe afrontar es dotarlas de facilidad de uso con objeto de hacerlas amigables y cercanas al usuario. Las soluciones e interfaces que una red personal incorpore no deben ser comprensibles únicamente por expertos en tecnologías, sino que deben ayudar a todos los usuarios a afrontar de forma agradable y eficiente las tareas cotidianas.

Los usuarios disponen de una gran cantidad de dispositivos, muchos de los cuales llevan consigo en su día a día. Bien sea por requerir configuraciones tediosas, bien porque los dispositivos no comparten las mismas tecnologías de comunicación, bien porque tienen un gran número de ellas y no se sabe cuál es la más adecuada en cada ocasión o bien porque los nodos no se detectan entre sí, la transferencia de información y la interacción entre ellos requiere en muchas veces de conocimientos avanzados. Permitir que los dispositivos se agrupen y comuniquen de forma automática sin intervención del usuario y se usen, siempre que sea posible, empleando interfaces visuales homogéneas, es uno de los grandes atractivos que una PN podría ofrecer. Al dotar estas funcionalidades, no se puede olvidar que la

seguridad y privacidad debe estar siempre presente, del mismo modo que lo está el usuario. Este es uno de los principales retos a afrontar.

La mejor manera de generar un sistema fácil de usar es que éste sea sencillo, pero que siga siendo capaz de realizar las tareas para las que ha sido diseñado, esto es, que cumpla con el resto de los requerimientos. En este sentido, un usuario debe comprender de forma clara la conformación de una PN y hacerse una idea mental de su estructura. Así, en caso de fallo o de un modo de operación imprevisto, el usuario podrá de forma autónoma identificar las razones y solventar el problema. Un ejemplo son las redes inalámbricas, cuya proliferación ha logrado que los usuarios dispongan una visión global de la metodología de acceso a la red, de forma que cuando detectan que no tienen conectividad a su punto de acceso, instintivamente comprueban que está encendido o reintentan introduciendo correctamente la clave de acceso. Aplicando esta forma de actuar a las PN, a pesar de que el sistema pueda operar de forma automática, el usuario siempre tendrá la última palabra.

Aunque más adelante se hace mención especial a la seguridad, desde el punto de vista de uso, los usuarios no son conscientes de los riesgos que corren al estar conectados. Siempre existirán usuarios maliciosos que tratarán de vulnerar la privacidad de los otros. En la mayor parte de las ocasiones, los sistemas de seguridad son tan complejos que el usuario, abrumado por ellos, prefiere deshabilitarlos, ignorar los avisos o utilizar claves sencillas. En esas situaciones se confirma la máxima que dicta que el eslabón más débil de la cadena de confianza suele ser el propio usuario. Es por esto que un diseño seguro, pero sencillo es crucial [3-5], de forma que se extienda su uso.

La implementación de las soluciones que hagan frente a los requerimientos identificados hasta ahora, no debe suponer un impedimento en hacer de las PN una solución escalable. Por otro lado, al ser el usuario nómada por naturaleza, su PN también lo será. Las mejoras en movilidad hoy en día están asociadas al consumo energético, es decir, la duración de las baterías determina el tiempo máximo que un usuario puede desplazarse sin tener que conectarse a la red eléctrica. Por tanto, la eficiencia energética está vinculada a tener una buena experiencia de uso. Algunas de las variables que la determinan son las propias características de los dispositivos (pantalla, etc.) y las metodologías de comunicación que empleen.

2.2.2. Seguridad, confianza y privacidad

Como se ha comentado anteriormente, el uso de una PN y la opinión que el usuario tenga de ella, depende en cierta forma de la confianza que ésta pueda proporcionarle. Sin embargo, las redes son vulnerables y más aún las móviles, inalámbricas y ad-hoc, en las que el usuario, si no es precavido, interacciona con numerosos elementos desconocidos [6]. Algunos de los ataques más comunes que se sufren según el nivel de la pila de protocolos al que se orientan se muestran en la tabla 2.1.

Es por esto que el mayor reto de las PN no es el diseño de nuevos algoritmos y protocolos de seguridad. Existen ya definidos gran número de ellos, en los que la seguridad de una PN se puede apoyar. El desafío consiste en dotar de un modelo de confianza entre personas, sus dispositivos y las redes sobre las que operan. Dicho modelo debe presentar la robustez

Tabla 2.1: Ejemplos de ataques según el nivel de la pila de protocolos

Nivel	Ataque
Multi-capas	Suplantación de identidad, troyanos, denegación de servicio (DoS, <i>Denial of Service</i>), hombre en el medio, repetición
Aplicación	Repudio, datos corruptos
Transporte	Apropiación de sesión, DoS por SYN
Red	Inundación, agujero de gusano (<i>wormhole</i>), agujeros negros (<i>blackhole</i>), consumo de recursos, revelación de la posición
Enlace	Análisis de tráfico, monitorización, debilidad protocolo, alteración dirección
Físico	Interferencia, escucha, intervención de comunicaciones

necesaria para garantizar la autenticidad e integridad de las relaciones, pero sin olvidar los aspectos mencionados asociados con la facilidad de uso [7].

La digitalización de la información se ha convertido en un aspecto cotidiano en el mundo actual. La información digital, unos y ceros, se trata y transmite de la misma forma independientemente de lo que represente. Se hace por tanto necesario añadir entropía al conjunto de bits en el que se han convertido los datos generados como parte de las actividades realizadas, para protegerlos y evitar su rastreo. La PN incluirá los mecanismos necesarios para dotar de confidencialidad no solo a las comunicaciones, sino también al almacenamiento y procesamiento de la información.

Otro aspecto a tener en cuenta en términos de seguridad es el intrusismo que supone el poder conocer la identidad de las personas. Los humanos suelen realizar las mismas tareas de forma repetitiva y llevar consigo los mismos dispositivos. Estos dos aspectos hacen factible la identificación. El primero es difícilmente evitable. Sin embargo, se puede actuar sobre la forma en la que funcionan los dispositivos. En cualquier comunicación inalámbrica la dirección a nivel de enlace o un identificador de nivel físico son expuestos. Evitarlo permitiría ayudar a tratar de mantener el anonimato. A pesar de que llevar este paradigma al extremo es prácticamente imposible, las PN deben encontrar una solución de compromiso.

En términos generales, se pueden definir dos grandes metodologías que agrupan las diversas formas de atajar los riesgos y problemas de seguridad a los que las redes se enfrentan. Por un lado, están aquellas soluciones que tratan de prevenir y de otro, las que reaccionan ante los ataques. Las soluciones empleadas en las redes tradicionales tratan de ser proactivas y evitar cualquier posible intromisión, aunque siempre incorporan sistemas de respaldo con los que detectar y solventar aquellos agujeros de seguridad que no se hayan logrado cerrar.

En esas redes, una tercera entidad de confianza (TTP, *Trusted Third Party*) certifica las relaciones entre sus miembros. Sin embargo, considerando las características de las redes ad-hoc, es difícil plantear esa figura. La diversidad de soluciones existentes para dar res-

puesta a las necesidades de comunicación en las redes ad-hoc, tal como se apunta en el apartado 2.4.1, hace que sea prácticamente imposible definir una arquitectura de seguridad común [8]. Además, las propuestas de comunicaciones por defecto no incorporan métodos para asegurar las transferencias, teniendo que requerir adaptar soluciones de seguridad dependiendo del método de encaminamiento que se emplee [9-13]. Queda por tanto reflejado que las PN deben proporcionar una solución integral que sea tanto válida para las comunicaciones de corto alcance, en el entorno cercano del usuario, como las remotas.

Otro aspecto a tener en cuenta es la posible pérdida de los dispositivos. Todo dispositivo tendrá datos de usuario entre los que se incluirán credenciales de acceso. Las PN deben tratar de minimizar el impacto de esta circunstancia.

En resumen, el modelo de seguridad que se implemente debe tener en cuenta a quien va dirigido y no obviar qué es lo que protege, es decir, un entorno móvil, dinámico y ubicuo. Este modelo, para operar eficientemente y ser aceptado por los usuarios, debería estar integrado en el núcleo de soluciones que sustenten la PN y, en la medida de lo posible, garantizar las cuatro máximas de la seguridad: confidencialidad, autenticación, integridad y no repudio.

2.2.3. Comunicaciones ubicuas

Puesto que las PN soportan las comunicaciones entre los nodos de un usuario independientemente de su localización, su disponibilidad y sus características, los mecanismos de comunicación que se implementen deben soportar estas condiciones. Así, el conjunto de necesidades que seguidamente se introducen no debe sorprender.

Las PAN están formadas por una gran variedad de dispositivos con unas características y funcionalidades muy diferentes, que van desde su propia apariencia externa, pasando por la capacidad de cómputo e interfaces de interacción, hasta las interfaces de comunicaciones. El soporte a esa diversidad, especialmente en comunicaciones, no está resuelto de forma integral.

Los nodos no se mantienen siempre dentro de la PAN, sino que se conectan y desconectan dependiendo de las necesidades del usuario. La propia agrupación de nodos se genera y destruye de forma espontánea. Además, en esos casos, no se puede confiar en la infraestructura para proveer la conectividad. Por tanto, se requieren metodologías de comunicación especiales que habiliten el enlace entre los miembros de la PAN en cualquier situación.

La PAN se limita a dominio próximo al usuario, pero las PN extienden el concepto sin limitación geográfica. Dependiendo del entorno y la aplicación a la que se acceda, se requiere una mayor área de cobertura, un mayor rendimiento o una mayor eficiencia energética. Por tanto, para dar respuesta a estas necesidades los terminales deben incorporar múltiples tecnologías de acceso inalámbrico y gestionarlas de forma inteligente según el entorno. Así, por ejemplo, los terminales incorporan interfaces de acceso a redes como *Global System for Mobile communications* (GSM)/*General Packet Radio Service* (GPRS) o *Universal Mobile Telecommunications System* (UMTS), empleadas en los escenarios de comunicaciones con mayor amplitud geográfica, y tecnologías como Bluetooth o Institute of Electrical and Electronics Engineers (IEEE) 802.15, orientadas al uso dentro de la celda personal. En

el rango intermedio, picoceldas y microceldas, se emplean soluciones sobre IEEE 802.11 e IEEE 802.16.

Es labor de la PN proporcionar los mecanismos que permitan al usuario realizar la configuración y gestión de toda esa variedad de interfaces de comunicación de forma transparente, siempre ofreciéndole las alternativas que mejores condiciones proporcionen (una o varias agregando tráfico), tratando de hacer realidad el paradigma “Siempre conectado de la mejor manera” (*Always Best Connected*) [14]. El lidiar con esa diversidad de tecnologías de comunicaciones en un entorno mayoritariamente basado en el protocolo *Internet Protocol* (IP) obliga también a adaptar los flujos no convencionales.

Adicionalmente, esa gestión incluirá el control de los traspasos tanto horizontales como verticales que se produzcan en un entorno tan cambiante como el de un usuario en movilidad. En la literatura existen soluciones estándares de movilidad entre redes como *Mobile IP* (MIP) [15, 16] o *Network Mobility* (NEMO) [17], además de que cada red internamente incluye sus propios métodos de traspaso. Sin embargo, en ninguna de ellas soporta de forma nativa la gestión de la conexión simultánea e inteligente a múltiples redes [18, 19].

Hacer frente a todas estas cuestiones de forma independiente en cada nivel de la pila de protocolos de comunicaciones puede provocar la toma de decisiones incorrectas. Dentro de una PN, considerando la flexibilidad que la caracteriza, quizás se debiera romper el modelo tradicional de capas aisladas y afrontar el diseño planteando soluciones que empleen estadísticas y métricas de diferentes niveles y las gestionen de manera conjunta. De esta forma, la detección de un canal de comunicaciones de baja calidad, adelantaría la aparición de pérdidas de paquetes en la transmisión y permitiría incluir los mecanismos de control de errores que proporcionaran una mayor robustez al canal. Los requerimientos que esta metodología de operación podría solventar están muy ligados con aquellos asociados a la adaptabilidad al contexto.

Recapitulando, se requiere que la PN ofrezca un entorno de red con soporte a la movilidad, que se configure y organice por sí solo y donde la gestión de las comunicaciones sea lo más transparente posible para el usuario.

2.2.4. Gestión y provisión de servicios

Las redes proporcionan acceso a los servicios y aplicaciones que, en última instancia, son lo que los usuarios consumen. La misma diversidad que se ha apuntado en cuanto a tecnologías de acceso se presenta, quizás ampliada, en posibilidades de implementación y provisión de servicios [20, 21]. Por tanto, parte de las afirmaciones que sustentan los requerimientos relacionados con la heterogeneidad a nivel de comunicación se pueden extender al nivel de servicio.

A nivel de servicio el rol de usuario, consumidor o proveedor, implica diferentes necesidades. Para el primer caso, el usuario se limita a la búsqueda y utilización de los servicios. En este sentido, esos servicios usualmente están disponibles en el propio terminal o bien son ofrecidos por proveedores externos. En este caso, la heterogeneidad antes apuntada no sólo se restringe a las tecnologías de creación y provisión de servicios, sino que también existe en metodologías de asignación de nombres. Insistiendo en la facilidad de uso, la arquitectura de servicios de una PN debería incluir mecanismos de traducción y adaptación de nom-

bres, que ligados a una plataforma integral de almacenamiento y búsqueda de servicios, supondría una mejora notable en la experiencia de uso.

Por otro lado, considerando la provisión, los servicios normalmente proporcionan sus propios clientes de acceso. Así, tras la búsqueda y elección de uno de los servicios será el proveedor quien gestione el acceso. No obstante, en aras de garantizar el soporte a la movilidad y la continuidad de las sesiones en aquellos servicios que no lo incorporen, deberá ser la plataforma de servicios que se diseñe para la PN la que incorpore esta funcionalidad. Por ende, la fiabilidad y la QoS podrán ser delegadas en la propia PN.

En el caso que el usuario quiera crear sus propios servicios, es necesario que la plataforma personal ofrezca una metodología clara e intuitiva. El lenguaje natural o el reuso de componentes conocidos pueden ayudar al usuario a extender las funcionalidades de su red.

2.2.5. Adaptabilidad al contexto

Se puede considerar el contexto de un objeto, ya sea un dispositivo, una red o una persona, como la información asociada a su entorno o situación. La influencia que el contexto puede tener en el comportamiento de ese objeto, le dota de un especial interés. Así, cuanta mayor información se disponga, mejor se podrá adaptar el funcionamiento a las circunstancias que lo rodean.

Trasladado este concepto al entorno personal, el contexto de cualquier objeto incluye una constante, el usuario. No sólo los datos provenientes del entorno de éste deben ser empleados para ajustar el funcionamiento de sus dispositivos, sino que éstos serán revisados en función de las preferencias del usuario, entre las que se pueden incluir las exigencias en cuanto a coste o QoS.

Dotar a los dispositivos de la inteligencia que permita usar toda la información disponible para adaptarse tanto a su propio contexto como al del usuario, es otro gran reto al que las PN deben hacer frente.

Adicionalmente, ya se ha señalado que los dispositivos de un usuario no solo están en sus proximidades, ni se mantienen constantes, sino que se encuentran distribuidos por los lugares donde lleva a cabo sus actividades. Conseguir la ubicuidad en el acceso a la información de contexto y plantear la arquitectura que lo proporcione se presenta como otra necesidad que las redes personales deben resolver [22].

2.3. Requerimientos de una federación de redes personales

El usuario creador de servicios suele querer compartirlos con aquéllos que tengan interés en él. Este es el origen de las colaboraciones entre PN, constituidas a partir de la agrupación de varios usuarios con intereses y objetivos comunes, que por sí solos no pueden acometer.

Como extensión de una PN, las PN-F comparten los requisitos planteados anteriormente, como por ejemplo la configuración, organización y mantenimiento autónomo. No obstante, plantean nuevos y complejos retos [23].

El primero de ellos consiste en la gestión de las relaciones entre los miembros y los recursos que comparten. Queda pendiente por tanto determinar la forma más óptima de llevarlo a

cabo, bien de forma centralizada, distribuida, colaborativa, etc. Por tanto, se deben definir los mecanismos que rijan los procesos de creación y participación dentro de las PN-F. Así, la especificación de una PN deberá ser capaz de integrar las modificaciones que se incluyan.

Pero antes, los usuarios deberán determinar qué comparten y las políticas de acceso que otorgan a los potenciales colaboradores. Autenticar tanto a los usuarios como garantizar la disponibilidad de aquellos recursos que se publicitan sólo a los usuarios o dispositivos autorizados es otro reto derivado del anterior.

En este sentido, el concepto de PN-F debe ser escalable, ya que el número de participantes no se fija de antemano. Es más una misma PN podrá colaborar en diferentes grupos. La solución que se proponga para la PN-F debe tratar de mantener la QoE que el usuario tiene dentro de su propia PN y no verse afectada por la aparición de otras.

2.4. Iniciativas relacionadas con las redes personales

Muchas y muy diversas iniciativas han surgido en el ámbito de las comunicaciones personales inalámbricas tratando de dar respuesta a las necesidades descritas. Sin embargo, la mayoría tratan cada uno de los aspectos de forma independiente en lugar de tratar de proporcionar una solución completa que resuelva de forma integrada todas las cuestiones relacionadas con las PN.

A continuación se enumeran algunos de estos trabajos que bien sólo han analizado los requerimientos de las comunicaciones personales desde el punto de vista de especificación teórica o bien han completado dichos estudios construyendo plataformas que permitan validar los diseños planteados.

Señalar que en la siguiente relación no se incluyen los proyectos IST MAGNET [24] y MAGNET Beyond [25], pues los trabajos realizados en esta tesis han surgido de la colaboración dentro de estos proyectos y, por tanto, se reflejan en los capítulos posteriores. Por la misma razón, tampoco se incluye el proyecto mIO! [26], perteneciente al subprograma de apoyo a Consorcios Estratégicos Nacionales de Investigación Técnica (CENIT). Algunas de las soluciones planteadas en este proyecto han sido empleadas para extender y validar nuevas visiones de las PN, más allá del enfoque presentado dentro de los proyectos MAGNET.

Antes de proceder resaltar que en paralelo con la ejecución del proyecto MAGNET Beyond, alguno de los miembros del consorcio participaron en iniciativas nacionales en la misma línea de investigación. El proyecto *Personal Networking Pilot 2008* (PNP 2008) [27] dentro del programa de investigación holandés *Freeband Communication* es una muestra de ello. Este proyecto presentaba un objetivo similar al de MAGNET Beyond, buscando demostrar el concepto de la PN en entornos reales e introducir las relaciones entre redes. Este este sentido ambos proyectos se retroalimentaron con propuestas de uno y otro, motivo éste por el que tampoco se ha incluido en el listado de trabajos previos relacionados.

2.4.1. Redes móviles ad-hoc

Una red ad-hoc se puede definir, de manera genérica, como un conjunto de nodos autónomos que se agrupan de manera dinámica y espontánea sin que tenga que existir un

elemento centralizador ni una infraestructura subyacente [28, 29]. Las comunicaciones entre los diferentes componentes de la red se llevan a cabo mediante enlaces inalámbricos. Los nodos, además, tienen la capacidad de moverse libremente y de manera arbitraria, con lo que la topología de la red puede variar sustancialmente, de manera poco predecible. Tanto es así que dos nodos cualesquiera no tienen por qué poder comunicarse a través de un enlace directo. En tal caso, serán el resto de los dispositivos próximos a ellos los que redirijan los paquetes que se envían para alcanzar su destino.

Como concepto se originó hace varias décadas con un propósito militar y no fue hasta mediados de la década de los noventa cuando el mundo académico empezó a mostrar interés en el tema. Desde entonces la evolución ha sido vertiginosa asentándose como un área de investigación relevante dentro del mundo de las comunicaciones inalámbricas. La labor de estandarización de los protocolos de encaminamiento para redes ad-hoc se realiza dentro del grupo de trabajo Mobile Ad hoc NETworks Working Group (MANET). Ante las numerosas propuestas existentes, dentro de ese grupo se ha decidido limitar el número de protocolos a especificar y desarrollar, centrándose en un protocolo por cada una de las dos grandes familias, reactivos y proactivos, definiéndose dos nuevos términos, protocolo reactivo MANET (RMP, *Reactive MANET Protocol*) y protocolo proactivo MANET (PMP, *Proactive MANET Protocol*). Las implementaciones específicas seleccionadas para éstos son *Dynamic MANET On-demand Routing* (DYMO) [30] y la segunda versión de *Optimized Link State Routing Protocol* (OLSR) [31, 32]. El grupo de trabajo MANET presta también especial atención a *Open Shortest Path First* (OSPF) [33], colaborando en todos aquellos puntos que involucren entornos en movilidad.

Además del encaminamiento, existen otras áreas dentro de las redes ad-hoc que han sido objeto de frecuentes estudios, como la difusión ordenada a todos los componentes de la red [34, 35] y la seguridad [36, 37].

La propia idiosincrasia de las redes ad-hoc hace que se puedan constituir en situaciones donde configurar redes tradicionales sería imposible. Esto abre un gran abanico de potenciales aplicaciones para ellas. De hecho, se pueden considerar la tecnología idónea generar una PN dado que ofrecen configuración, organización y mantenimiento autónomo. Serán, por tanto, como se verá en capítulos posteriores un importante elemento en la construcción de una PN y dotar de comunicación ubicua a los nodos y dispositivos de usuario.

2.4.2. Computación y comunicación ubicua

Mientras que el *Book of Visions* [38] del Wireless World Research Forum (WWRF) y su visión de las redes inalámbricas se generó principalmente a partir de aportaciones europeas, la computación y comunicación ubicua es un concepto cuya evolución ha sido guiada principalmente por la industria estadounidense. Originado bajo la idea de que los procesos de cálculo deberían ejecutarse continuamente en segundo plano e interactuar solo cuando sea necesario con los usuarios, la computación ubicua permitiría al usuario llegar a abstraerse de los sistemas y considerarlos como una ayuda en su día a día. De esta forma, los dispositivos, analizando el entorno del usuario, percibiendo los cambios en él y cooperando entre ellos, actuarían inmediatamente adaptándose a las preferencias y necesidades de aquéllos.

Sin embargo, la computación ubicua y el concepto de PN difieren en un importante

matiz. Mientras que la computación ubicua considera cualquier dispositivo o nodo, incluso un portátil, como un mero instrumento que sirve a cualquier usuario y que éste no debería poseer ni transportar pues en cualquier lugar puede encontrar las capacidades que le ofrecen, la PN sí considera la propiedad de los objetos y su uso personalizado.

A pesar de esta sibilina diferencia, la investigación realizada en el ámbito de la computación y comunicación ubicua es de utilidad para definir una PN. La información recogida por sensores y redes alrededor del usuario, su procesamiento y posterior uso sí proporciona respuesta a las necesidades planteadas para la PN.

2.4.3. Wireless World Research Forum

El WWRF [39] surge en 2001 y en ella participan tanto fabricantes, operadores de red, proveedores de servicio como instituciones académicas y de investigación. El objetivo del WWRF es proporcionar una visión de futuro y describir las líneas maestras y tendencias de investigación en el campo de las comunicaciones inalámbricas. Adicionalmente, supone una plataforma de discusión y difusión de los resultados de los trabajos que se vayan realizando, habilitando los medios para contribuir en European Telecommunications Standards Institute (ETSI), 3rd Generation Partnership Project (3GPP), Internet Engineering Task Force (IETF), International Telecommunication Union (ITU) y otros organismos de estandarización.



Figura 2.1: Modelo de referencia Multi-Esfera [38]

Producto del trabajo en el WWRF es el *Book of Visions* [38]. En este reporte se reúnen las ideas de diversos expertos en el campo de los sistemas de comunicaciones inalámbricas y adelantan los retos para el desarrollo de las siguientes generaciones. Entre otras propuestas se definió el modelo Multi-Esfera (*MultiSphere*), representado en la figura 2.1, que dividía los sistemas en múltiples esferas o capas. La capa más interna incluye la PAN que conecta los dispositivos portátiles de un usuario. La siguiente capa incluiría el conjunto de nodos con los que se pueden comunicar aquellos pertenecientes a la PAN. La tercera capa estaría formada por las redes cercanas pertenecientes a otros usuarios, siendo la capa más externa la formada por redes complejas de operador (p. ej. GSM/GPRS o UMTS) y las comunicaciones con el resto del mundo digital, como Internet.

Las PN encajan parcialmente en el modelo Multi-Esfera, como se verá a lo largo de esta tesis. En este sentido, las PN toman prestado algunas ideas como la heterogeneidad en

dispositivos, tecnologías de comunicaciones y servicios, la auto-configuración y la adaptación. No obstante, indicar que el modelo proporcionado por el WWRF no cubre todas las necesidades previstas para las PN, como son la seguridad y la privacidad o la interacción entre las personas y sus dispositivos.

2.4.4. Ambient Networks

Ambient Networks (AN) [40, 41] es un proyecto IST financiado dentro del 6º Programa Marco de la Unión Europea (UE), surgido a partir de la Wireless World Initiative (WWI) del WWRF. Su principal objetivo era la creación de soluciones de red escalables y económicas aplicables a sistemas móviles inalámbricos de siguiente generación, que permitieran la provisión de servicios de valor añadido para todos.

Hoy en día existen diferentes tipos de redes a disposición de los usuarios y nuevos tipos se despliegan, con frecuencia, en cortos períodos de tiempo. AN busca habilitar la interoperabilidad entre redes heterogéneas de forma natural y transparente. La identificación de un conjunto de funcionalidades comunes genera un plano de control único que puede ser desplegado como un componente integral de las futuras redes o como un añadido a las redes actuales. Adicionalmente, abstrae las diferencias en los planos de conectividad y define un conjunto de primitivas genéricas para ser empleadas por los servicios y aplicaciones independientemente de la red sobre la que se ejecuten.

En este sentido, el proyecto persigue la composición dinámica de redes, lo que posibilita el acceso a las capacidades de cualquier red mediante acuerdos bilaterales establecidos bajo demanda. Las soluciones definidas soportan el vínculo entre las redes de los usuarios y la infraestructura de interconexión, sin olvidar la importancia de la comunicación dentro de esas redes y el cumplimiento de los niveles de fiabilidad y QoS requeridos.

Es por esto que la inclusión de algunos de los trabajos realizados en AN, aunque estuvieran orientados más al plano de operador, pueden permitir a las PN formar parte de estas nuevas redes cooperativas originadas bajo el paraguas de AN.

2.4.5. PACWOMAN

Power Aware Communications for Wireless Optimised Personal Area Network (PACWOMAN) [42] es un proyecto IST perteneciente al 5º Programa Marco de la UE, cuyo trabajo se centró en el desarrollo de comunicaciones ad-hoc en WPAN, aunque en él también se llevaron a cabo trabajos sobre tecnologías de nivel físico como *Ultra Wide Band* (UWB).

PACWOMAN define una arquitectura de referencia en tres niveles [43]. La PAN es el primero de ellos, donde los dispositivos personales pueden comunicarse entre ellos. La PAN tiene identidad propia y en el caso más simple operaría independientemente de cualquier otra red. El siguiente nivel lo constituye la red de área comunitaria (CAN, *Community Area Network*), que está constituida por las PAN próximas de usuarios que desean interactuar entre sí. La comunicación entre ellas se realiza empleando soluciones de encaminamiento inalámbrico ad-hoc, lo que permite la formación espontánea de redes en cualquier instante y lugar, manteniendo la integridad dentro de la PAN. Para completar la estructura, se define un tercer nivel, WAN, que habilita la comunicación de la PAN con dispositivos remotos.

Otro de los resultados de PACWOMAN fue el desarrollo de soluciones de nivel de enlace y *Medium Access Control* (MAC) para el entorno PAN. Gracias a ellas se trata de forma diferente la comunicación mediante tecnologías radio de baja velocidad de transmisión de datos (LDR, *Low Data Rate*) y de alta velocidad de transmisión de datos (HDR, *High Data Rate*). Por ejemplo, las especiales características de los dispositivos en las que se implementan las primeras (sensores y pequeños dispositivos de usuario), hacen que las tecnologías LDR deban tener especial consideración al consumo energético.

De nuevo, en este caso los trabajos realizados en PACWOMAN, especialmente los enfocados a la heterogeneidad de las comunicaciones y dispositivos y a la comunicación ubicua, son de interés para el desarrollo del concepto de PN.

2.4.6. SHAMAN

Secure Heterogeneous Access to Mobile Applications and Networks (SHAMAN) [44] es otro proyecto IST perteneciente al 5º Programa Marco de la UE que proporciona una arquitectura de seguridad para la PAN basada en un modelo de confianza [45], que describe la relación de seguridad básica entre los dispositivos de una PAN. Cada dispositivo de usuario podrá únicamente ser usado por aquéllos que el propietario disponga según sus políticas de seguridad. La plataforma de seguridad definida engloba tanto la comunicación local dentro de la PAN como el acceso a través de la infraestructura.

Los dispositivos se clasifican dependiendo de la relación de confianza que tengan con sus homónimos. En este sentido se definen tres tipos, dispositivos de usuario que son confiables entre sí, dispositivos de terceros también de confianza y dispositivos externos que no son de confianza. La confianza se sustentan en una autoridad de certificación (CA, *Certification Authority*) personal localizada en uno de los dispositivos de usuario y que emite certificados a los miembros de la PAN del usuario [46].

Si PACWOMAN proporcionaba una base sobre la que sustentar las comunicaciones, SHAMAN aporta un modelo de seguridad que cubre parte de los requerimientos de seguridad observados para las PN. La solución final irá en la línea de combinar lo mejor de ambas propuestas en una única solución.

2.4.7. MobiLife

En 2004, con el propósito de investigar nuevas tendencias en servicios y aplicaciones móviles se lanzó, dentro del 6º Programa Marco de la UE, el proyecto IST MobiLife [47, 48]. El objetivo estratégico era innovar en la provisión de servicios en movilidad, considerando para ello las condiciones en las que los usuarios consumidores de dichos servicios se encontraban. Adicionalmente los nuevos servicios deberían hacer uso extensivo de las nuevas capacidades de los sistemas de tercera generación y posteriores.

En el día a día de un usuario, éste emplea una gran diversidad de dispositivos y redes e interactúa de forma muy diferente con ellos dependiendo de las condiciones de su entorno. Incluso el propio usuario puede adoptar diferentes papeles e interactuar con diferentes grupos de personas a lo largo del día. El reto de MobiLife era gestionar de forma transparente toda esta complejidad. Para ello, el proyecto basó su trabajo en una filosofía centrada en el usuario tratando de dar respuesta a las necesidades de su vida cotidiana proveyendo

soluciones seguras, adaptables y conscientes del contexto, siempre en un entorno inalámbrico móvil.

Las soluciones de MobiLife se estructuraron en dominios de interacción, desde el entorno personal al global, pasando por grupos de usuarios. En todos ellos, el contexto y las interfaces multimodales estaban presentes, buscando proporcionar un acceso transparente a los servicios independientemente del dominio.

La visión del MobiLife está en sintonía con el concepto de PN, como red inalámbrica centrada en el usuario.

2.4.8. Entorno Personal Distribuido

Dentro del programa de orientado a las comunicaciones móviles y personales del Virtual Centre of Excellence (VCE) del Reino Unido [49], se acuña el término entorno personal distribuido (PDE, *Personal Distributed Environment*) [50, 51]. PDE ofrece un enfoque muy similar al de las PN. El programa va más allá de una simple visión y se trata de concretarla en una arquitectura y su posterior implementación.

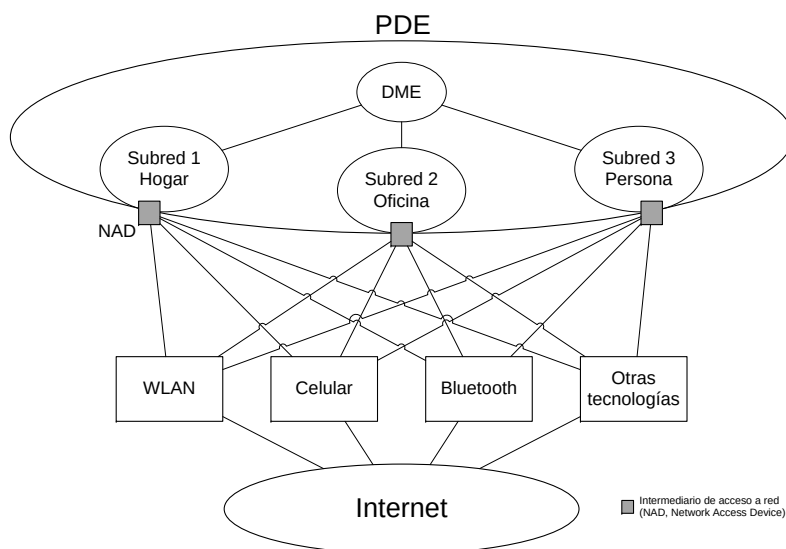


Figura 2.2: Modelo de red según PDE

El PDE consiste en un conjunto de dispositivos y servicios de usuario, tanto locales como remotos [52]. El modelo implantado se representa en la figura 2.2. En el centro de un PDE está un servidor PDE donde se ejecuta una entidad gestora de dispositivos (DME, *Device Management Entity*). El servidor DME es básicamente un servidor con una base de datos de todos los dispositivos que pertenecen a un usuario. Para mantener actualizada esta información, todo dispositivo se mantiene en contacto con el servidor PDE remitiendo los cambios en su localización, capacidades y servicios. La comunicación entre el servidor PDE y los dispositivos puede ser directa o a través de nodos pasarela, sobre un canal tanto seguro como inseguro. El servidor PDE hace de intermediario entre dispositivos en el acceso a los servicios.

Aunque PDE se centra principalmente en soluciones a nivel de servicio, también cubre aspectos de nivel de red. Los dispositivos de un mismo PDE se pueden comunicar entre ellos usando tecnologías de comunicaciones de red local formando pequeñas redes. Ejemplos de estas redes son las PAN, las red de área corporal (BAN, *Body Area Network*) o las redes del hogar o la oficina. Estas redes se conectan entre sí mediante los denominados intermediarios de acceso a red (NAD, *Network Address Device*).

El PDE no define una metodología de comunicación dentro de cada subred, operando sobre entornos estándar. Tampoco proporciona una solución de seguridad común, recayendo la aplicación de las políticas de seguridad en las relaciones en el PDE en el servidor DME.

En definitiva, el PDE no proporciona un entorno homogéneo. Así, aunque mantener las soluciones de comunicaciones existentes sin modificación se puede considerar a priori un beneficio, hace que la heterogeneidad existente pueda dificultar la interacción entre dispositivos y la movilidad de estos de una subred a otra. Además, esta diversidad hace que sea el propio usuario quien tenga que conocer y abordar las tareas de configuración de cada una de ellas.

2.4.9. MyNet

El proyecto MyNet [53-55] surge de la colaboración entre el Computer Science and Artificial Intelligence Laboratory (CSAIL) del Massachusetts Institute of Technology (MIT) y Nokia, cuyo objetivo es el estudio y el desarrollo de una arquitectura de red y las aplicaciones y herramientas que permitan la creación de redes virtuales seguras de forma simple.

User Information Architecture (UIA) [56] y *Unmanaged Internet Protocol* (UIP) [57] son proyectos del MIT que se han tomado como base del trabajo en MyNet. UIP combina la gestión autónoma de las redes ad-hoc con la escalabilidad de IP. Para ello genera redes virtuales superpuestas entre los dispositivos personales. Por su parte, UIA, se centra en habilitar la interacción total entre los dispositivos de diferentes personas. Los protocolos definidos en UIP son la base sobre la que sus

La UIA se fundamenta en dos principios: (a) la seguridad es independiente de la conexión física y (b) la confianza se genera sustentándose en las relaciones sociales entre los usuarios. Esto se logra asignando espacios de nombres (*namespaces*) privados y personales a los grupos de nodos, lo que facilita el establecimiento de redes sociales para el intercambio de recursos.

Estos dos proyectos nacen a raíz del trabajo de investigación en comunicaciones entre iguales (P2P, *Peer-to-Peer*), pero comparten ciertos aspectos comunes con las PN. La seguridad, la facilidad de uso, auto-configuración y gestión son algunas de ellas. En este sentido, con la orientación social que promulgan ofrecen un punto de vista muy interesante de establecer conexiones seguras entre los extremos de las PN, sin tener que usar una infraestructura de clave pública (PKI, *Public Key Infrastructure*). De forma natural, los usuarios extenderán la confianza y determinarán con quienes compartirán sus recursos y qué accesos les darán.

2.4.10. P2P Universal Computing Consortium

El consorcio *P2P Universal Computing Consortium* (PUCC) [58, 59] es una colaboración entre universidades e instituciones académicas japonesas y algunas de las compañías más activas en Japón, como NEC, Toshiba y NTT DoCoMo. El objetivo de PUCC es desarrollar una plataforma de comunicaciones que permita comunicaciones P2P de forma transparente para soportar los intercambios entre dispositivos ejecutando servicios ubicuos.

La pila de protocolos más comúnmente empleada para conectarse a Internet es *Transmission Control Protocol* (TCP)/IP. No obstante, los dispositivos en el entorno del usuario suelen estar equipados y emplean tecnologías de comunicaciones inalámbricas de corto alcance, como Bluetooth, asociación de datos infrarrojos (IrDA, *Infrared Data Association*) o Zigbee, para establecer las PAN. El diseño de estas tecnologías no buscó el soporte TCP/IP, sino ofrecer otras capacidades a los usuarios.

Con objeto de extender las funcionalidades que soportan estas tecnologías PUCC plantea el uso de un nodo pasarela o *gateway* que posibilite la interacción de dispositivos que empleen diferentes tecnologías y protocolos.

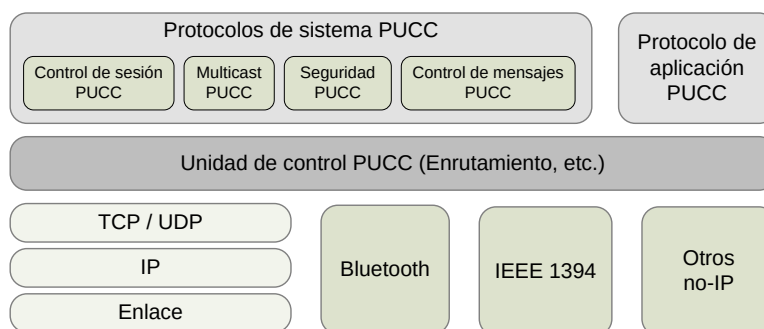


Figura 2.3: Pila de protocolos de la plataforma PUCC

En la figura 2.3 se muestra la pila de protocolos propuesta en PUCC. A través de redes P2P superpuestas, y sin modificar las capas de red subyacentes, se proporciona comunicación entre las redes IP y no IP (p. ej. redes de sensores). Posteriormente, por encima de ellas, la plataforma de servicios integra todas las funcionalidades de alto nivel que se ofrezcan, incluyendo el descubrimiento y gestión de éstos, así como su seguridad.

2.4.11. Otras iniciativas

Existen otros múltiples proyectos que incluyen entre sus líneas de trabajos aspectos relacionados con las PN. *Universal Personal Networking* (UPN) [60] es uno de ellos surgido en el entorno de Siemens al principio de la década de los noventa. Por entonces, las WPAN eran un concepto casi desconocido y las WLAN estaban comenzando a aparecer. Los planteamientos de UPN se asemejan mucho al concepto de PN a pesar de las limitaciones tecnológicas existentes por entonces. Se focalizó en el desarrollo de PN, dispositivos e interfaces de usuario, pero empleando el soporte de la infraestructura de interconexión. Aunque realizado con anterioridad a la eclosión de Internet, este proyecto puso mucho esfuerzo en definir soluciones similares a las que más tarde se ofrecerían en Internet. No obstante, descuidaron los aspectos de seguridad.

Otra iniciativa, también de Siemens, es *Life Works* [61] que ofrecía un concepto visionario consistente en unificar la experiencia de comunicaciones de empresa y personales. Bajo el paraguas de LifeWorks, Siemens desarrolló productos buscando la convergencia entre las redes fijas y móviles y nuevos servicios para los usuarios a desplegar en los entornos móviles.

Los trabajos en esta dirección no se reducen a Siemens, sino que la práctica totalidad de la industria de telecomunicaciones muestra un cada vez mayor interés en esta área. No obstante, los esfuerzos se están dirigiendo más al ámbito profesional que al del propio usuario como individuo, si bien ambos están convergiendo en cierta manera.

IBM definió y demostró el concepto de núcleo móvil personal (PMH, *Personal Mobile Hub*) [62], que actúa como enlace de comunicaciones entre la PAN y la infraestructura de interconexión. El PMH permite controlar una PAN formada por un conjunto de dispositivos de usuario y conectarlos a servidores en la infraestructura. El demostrador de este concepto se basó en una aplicación vinculada al mundo sanitario, en la que se monitorizaba la frecuencia cardíaca y la presión arterial, generando alertas ante la superación de ciertos niveles considerados de riesgo. Es más, la aplicación también permitía controlar la correcta administración de la medicación y avisar al usuario o responsable en caso de problemas.

Centrándose en el entorno académico, es importante destacar el trabajo realizado por la Universidad de Illinois en Urbana-Champaign. Entre las soluciones para PN que ofrecen, *MOBILE grouPEd Device* (MOPED) [63] se erige como un sistema que expone al conjunto de dispositivos personales de un usuario ante Internet como una única entidad empleando una única dirección pública global. Esta dirección se asigna a un intermediario o *proxy* permanentemente accesible desde Internet y que tiene conocimiento de la composición de la agrupación de nodos y de cómo se conectan entre ellos y a Internet. En la terminología de MOPED, los dispositivos personales que se pueden conectar entre ellos forman lo que se denominan componentes. Un componente se puede conectar a Internet o al intermediario. Gracias a esta arquitectura, MOPED establece los medios para dar soporte a redes personales desde el punto de vista de encaminamiento, direccionamiento y movilidad, lo que deja aún por solventar otros detalles como la seguridad, el soporte a los servicios y la comunicación directa entre componentes.

Existen otros muchos proyectos o soluciones no tan ambiciosas como las anteriores que ofrecen alternativas para desarrollar o mejorar alguna funcionalidad de una PN. Por ejemplo, el proyecto *CoolTown* [64] de Hewlett-Packard (HP) aplica las tecnologías web para el desarrollo de plataformas que permitan al usuario de dispositivos inalámbricos interactuar con el entorno de forma ubicua. La publicación de la presencia de objetos o personas vinculadas a lugares e instantes de tiempo abre la puerta de numerosos servicios que conecten el mundo virtual con el real. El proyecto *Mobile People* [65] de la Universidad de Stanford dispone una solución de movilidad a nivel de aplicación. Consideran que los extremos de la comunicación son personas y no los propios dispositivos. Para lograr dar soporte a esta visión, introducen una entidad que lleva a cabo el seguimiento de la persona y gestiona cualquier aspecto relacionado con la movilidad, esto es, redirección de llamadas al dispositivo y localización correcta, adaptación del flujo de datos, protección de las comunicaciones, etc. Tanto *CoolTown* como *Mobile People* son dos proyectos cuyas comunicaciones están basadas en el soporte en la infraestructura de interconexión y no consideran la comunicación

local entre dispositivos y otros conceptos de las PN. No obstante, incluyen ciertas ideas y planteamientos de interés.

Para finalizar, mencionar que el 3GPP en la evolución hacia las redes totalmente IP (*All-IP Networks*) [66] considera entre sus casos de uso y escenarios, situaciones muy similares a las redes personales. De hecho, en las especificaciones se emplea el término “redes personales” (*Personal Networks*), como una red en la que una persona con sus dispositivos se desplaza entre diversas localizaciones que están interconectadas empleando tanto redes 3GPP como no 3GPP.

2.5. Resumen

Para finalizar en la tabla 2.2 se muestra una comparativa de cómo cada una de las iniciativas descritas responde a los diferentes grupos de requisitos definidos. Se observa que ninguno de los proyectos los engloba todos de manera simultánea, si bien algunos de ellos encuentran mejor respuesta en algunos y la suma de todos los esfuerzos podría dar soporte a una red personal.

Destacar que la adaptabilidad al contexto desde el punto de vista de usuario solo se trata desde MobiLife. La mayoría hace frente a las comunicaciones heterogéneas de una u otra manera, aunque no ofrecen una solución de seguridad integrada sino que se sustentan en procedimientos estandarizados.

Tabla 2.2: Comparativa de iniciativas relacionadas con las redes personales

	Facilidad de uso		Seguridad, confianza y privacidad		Comunicaciones ubicuas	Gestión y provisión de servicios	Adaptabilidad al contexto
Ambient Networks			✓		✓		
PACWOMAN	✓	✓	✓✓				
SHAMAN	✓	✓✓					
MobiLife	✓		✓		✓	✓	✓
PDE	✓		✓✓		✓✓		
MyNet	✓	✓	✓		✓		
PUCC		✓✓	✓✓		✓✓		
MOPED			✓✓				
PHM		✓	✓				

Capítulo 3

Hacia las redes personales

Independientemente de la dirección que la evolución tecnológica siga en los próximos años, existe el consenso de que las nuevas tecnologías deben no sólo adaptarse a las personas, sino enfocarse a mejorar su calidad de vida y experiencia de uso, eliminando la necesidad de conocer todos los aspectos técnicos subyacentes. El entorno inteligente estará, por tanto, centrado en el usuario. Dotar de ubicuidad, personalización y transparencia al acceso a la información por parte de los usuarios dejará de ser una utopía para convertirse en un requerimiento indispensable. Tradicionalmente los múltiples dispositivos de usuario han sido configurados y gestionados por el propio usuario, siendo las tareas que éstos realizan aquellas para las que han sido programados. No obstante, las nuevas tendencias de uso implican que deberán aprender de los requerimientos y preferencias de aquél y actuar de manera inteligente para aportarle la máxima satisfacción de uso. El objetivo a cumplir es adelantarse a las necesidades del usuario en cualquier lugar, momento o situación en la que pueda encontrarse.

Todos estos futuros escenarios se caracterizan además por la heterogeneidad, tanto en cuanto a tipos de dispositivos, como también en lo que respecta a la gran variedad de servicios que se ofrecerán a los usuarios. En este contexto, usar exclusivamente las soluciones de comunicaciones actuales no es suficiente para proporcionar un acceso multimodal y una interrelación transparente entre los dispositivos. Si a esto se unen las cada vez más exigentes demandas en términos de simplicidad en el empleo de los diferentes aparatos usados en el día a día por los consumidores (ordenadores personales, teléfonos móviles, reproductores multimedia, todo tipo de periféricos, etc.), se infiere la imperiosa necesidad de desarrollar nuevas soluciones, que, evitando las tediosas y usualmente costosas tareas de configuración, permitan mantener las funcionalidades ya disponibles y, en la medida de lo posible, incrementarlas.

La colaboración entre los diferentes dispositivos, personales y/o compartidos por otros usuarios o entidades puede habilitar la provisión de un conjunto más versátil y potente de servicios. Es más, la combinación coordinada de estos servicios generará otros más avanzados que darán respuesta a todas las necesidades y expectativas de los usuarios, al tiempo que mejorarán la experiencia de uso (p. ej. la visualización de contenidos del teléfono móvil en una pantalla de televisión, etc.). Estos servicios, como por ejemplo los servicios multimedia, demandan un alto ancho de banda y una notable QoS. La definición de nuevos

entornos colaborativos hará viable suministrarlos de forma adecuada, haciendo realidad la composición y orquestación de servicios en movilidad.

En este nuevo entorno, que se ha venido describiendo y en el cual se permite el acceso a una multitud de recursos, la seguridad debe ser un aspecto a tener muy en cuenta. Asegurar la integridad, autenticidad y privacidad de los datos del usuario en un entorno tan heterogéneo se convierte en un reto. Se puede, por tanto, afirmar que habilitar únicamente el acceso autorizado y restringido a los recursos es tan importante como dotar de la capacidad de interconexión a los diferentes nodos. Sin embargo, la gran variedad de dispositivos y servicios requiere la definición y uso de mecanismos que permitan superar las deficiencias de seguridad inherentes en la tecnología y dotar al usuario de un entorno con garantías.

Adicionalmente, no se debe menospreciar la relevancia del papel de aquellos aspectos relacionados con la eficiencia energética, puesto que será esta característica la que haga viable la escalabilidad y portabilidad de estas nuevas soluciones.

Hasta el momento, las soluciones propuestas en el área de las comunicaciones inalámbricas en el entorno personal han sido numerosas y variadas, pero sólo un grupo reducido de ellas ha tratado de dar una solución global e integrada a las cuestiones descritas con anterioridad. Entre todas ellas, las PN se postulan como la opción más adecuada, pues tienen su génesis en la investigación conjunta en comunicaciones ad-hoc centradas en el usuario, tal como se refleja en [38].

Uno de los objetivos de esta tesis es proporcionar una solución genérica que permita hacer realidad el paradigma de las PN. En este capítulo se realiza la descripción de la operativa de una PN, considerando la interacción entre los dispositivos de un único usuario. No obstante, por todos es conocido que las personas necesitan relacionarse unas con otras y que dichas relaciones les hacen ser quienes son y evolucionar en una u otra dirección. El mismo comportamiento se puede extender a las redes de comunicaciones, dando como resultado la PN-F, concepto que será tratado en profundidad en el capítulo 5.

3.1. Concepto de red personal

Considérese el concepto de computación ubicua combinado con un fuerte protagonismo del usuario; se tiene así una definición de PN. Sin embargo, obviando esa orientación al usuario, la computación ubicua comparada con las PN presenta notables diferencias. Desde la perspectiva de la computación ubicua, los elementos de computación se consideran equipamiento de carácter genérico al servicio del usuario, cuyo propósito es su uso compartido. Por el contrario, en las PN [67, 68] cada usuario dispone de su propio equipamiento que, interconectado, forma la red de dicho usuario. En este último caso, los dispositivos del usuario estarán personalizados, dotándolos de singularidad. No obstante, a pesar de estas diferencias no hay que olvidar que gran parte de los esfuerzos y resultados de la investigación en computación y comunicaciones ubicua se puede trasladar a las PN [69, 70].

La PN es un concepto novedoso que combina la inteligencia ambiental con una atención especial al usuario. El concepto de PN fue acuñado dentro del proyecto IST MAGNET [24], en el marco del cual se ha llevado a cabo parte del trabajo de esta tesis. Una PN ofrece auto-configuración y auto-organización de la red de dispositivos personales, independien-

temente de la localización geográfica y las capacidades de comunicación y movilidad. La idea subyacente es que los dispositivos pertenecientes a un usuario se organizan en una red personal segura y confiable de forma transparente, permitiendo su interconexión sin tener en cuenta su localización o la tecnología de acceso empleada. De esta forma, el usuario siempre tiene la red de dispositivos disponible para atender sus necesidades particulares. El conjunto de dispositivos personales que forman parte de esta red virtual reaccionará de forma inteligente ante los cambios en el entorno y contexto de dicho usuario. Adicionalmente, la PN debe estar preparada para compartir los recursos y servicios disponibles con otros usuarios que hayan sido autorizados, promoviendo la colaboración entre PN de diversos usuarios.

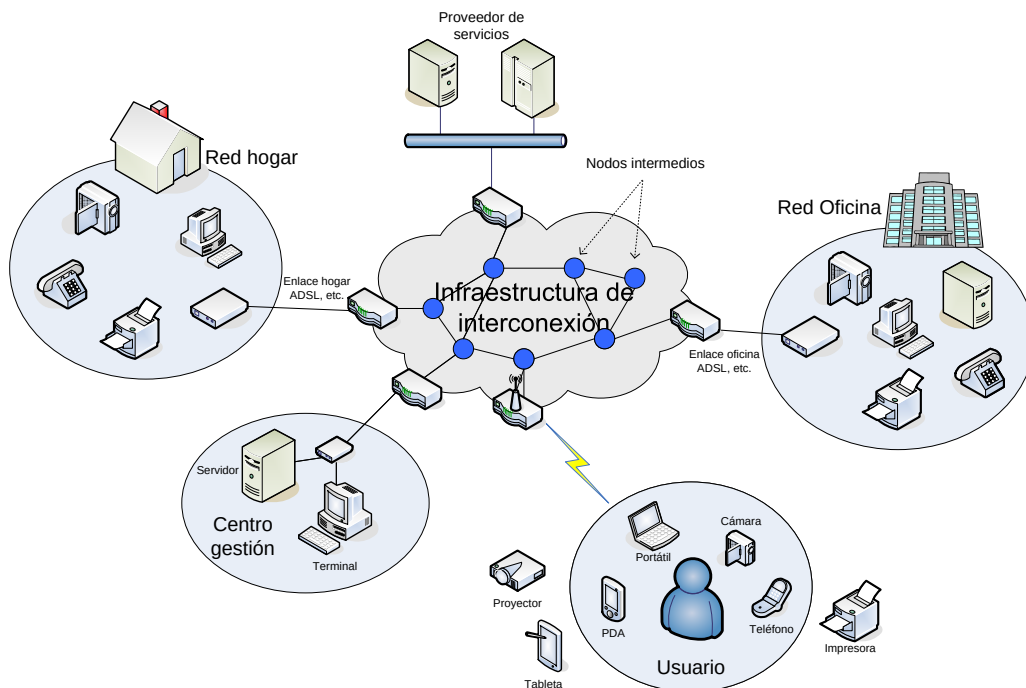


Figura 3.1: Ejemplo de una red personal

Desde el punto de vista de seguridad, una PN se define como la agregación privada de los dispositivos de un usuario, considerados como nodos o dispositivos personales, conformando una red virtual segura donde dispositivos vecinos se organizan de forma automática en *clusters*. En este caso, la PN se puede ver como un conjunto de dispositivos entre los que existe una relación de confianza. Tanto la seguridad como la privacidad se consideran características fundamentales de una PN, como también lo es la capacidad para auto-organizarse y adaptarse a la movilidad y cambios del entorno [71, 72].

Por otro lado, los nodos personales son oportunistas y se comunican empleando cualquier tecnología disponible. Como se ha comentado, se organizan en *clusters* que a su vez forman la PN (ver ejemplo mostrado en la figura 3.1). El *cluster* que se forma alrededor del usuario es un *cluster* especial denominado red privada del entorno de usuario (P-PAN, *Private Personal Area Network*) y está compuesto por sensores inalámbricos y otros dispositivos portátiles que el usuario porta consigo o de los que hace un uso muy frecuente. Las

conexiones entre los *clusters* de una PN se gestionan de forma transparente y son capaces de adaptarse a los cambios en la capa de acceso empleada. Usualmente estos enlaces se sustentan en la infraestructura desplegada, aunque si están próximos pueden comunicarse mediante enlaces radio directos. Las redes del usuario en el hogar, en la oficina o en el interior del coche son algunos ejemplos de estos *clusters*.

Las PN, además de salvaguardar la seguridad y la privacidad en los intercambios entre nodos, deben ser capaces de operar sobre cualquier tipo de red, bien ya existente y sobre la que se distribuyen diferentes servicios de operador, o bien generada explícitamente para un propósito particular. Se trata de redes dinámicas cuya composición, configuración y conectividad dependen del momento, lugar, preferencias y contexto de usuario, así como de los recursos disponibles.

Las PN se conciben para dar soporte a los usuarios en su día a día y, dada su naturaleza intrínsecamente personal, pueden proporcionar experiencias de uso más satisfactorias adaptándose a la situación actual del usuario teniendo en cuenta las preferencias de éste. Así, los servicios y aplicaciones que se ejecuten sobre una PN serán sensibles al contexto del usuario y de sus dispositivos. Este modo de operación no es de aplicación directa, sino que la información del contexto y el perfil de usuario deben hacerse accesibles a estos servicios. Es necesaria la consideración de un *middleware* que realice esta provisión de información y un eficiente acceso al contexto.

Recopilando las características más relevantes de una PN y resumiendo su operativa, hay que destacar que la complejidad resultante de la configuración y despliegue de una red, la sensibilidad al contexto y la seguridad y privacidad de la red quedan ocultas para el usuario final. Al operar sobre su PN, el usuario sólo tiene conciencia de los servicios disponibles en ella y en aquellos nodos vecinos que sean accesibles de forma confiable. En las siguientes secciones, se describirán en profundidad las soluciones diseñadas y desarrolladas para soportar las funcionalidades descritas.

Es importante señalar que, al contrario que en otras iniciativas que exploran de forma aislada las redes inalámbricas de área personal [73], las redes móviles ad-hoc [74] o la auto-configuración de redes [75, 76] centrándose en la optimización de cada entorno en particular sin tener en cuenta el resto, las PN siguen un enfoque integrado que engloba múltiples requerimientos de nivel de conectividad o enlace, de red, de servicio y de contexto, con el objeto de dar respuesta al objetivo planteado de proporcionar una red autónoma, auto-configurable y segura que sirva al usuario tanto para sus actividades personales como profesionales.

3.1.1. Terminología

La terminología empleada es el resultado de los análisis realizados durante el proyecto MAGNET, habiendo sido adaptados para ajustarse a la visión planteada en esta tesis. Los más comunes y relevantes usados en el presente trabajo se citan en la tabla 3.1, si bien en [77] se dispone de un glosario más amplio. La enumeración anterior es una lista de los conceptos más importantes y facilitará la lectura y el seguimiento de las descripciones que se realizarán en las siguientes secciones, aunque eventualmente se incorporará algún nuevo término según las necesidades.

Tabla 3.1: Terminología vinculada a las redes personales

Términos comunes	
Dispositivo (<i>Device</i>)	Cualquier entidad con capacidades de comunicación.
Nodo (<i>Node</i>)	Todo aquel dispositivo que implemente IPv6 [78] y/o IPv4 [79].
<i>Cluster</i>	Agregación dinámica de nodos y dispositivos personales circunscritos en un espacio geográfico y entre los cuales existe una relación de confianza mutua, que están conectados entre sí mediante una o varias tecnologías de comunicaciones y pueden comunicarse sin necesidad de hacer uso de otros nodos más que los propios nodos personales.
Red privada del entorno de usuario (<i>Private Personal Area Network</i>)	Una P-PAN es el <i>cluster</i> operando en torno al dueño de la PN. La privacidad en una P-PAN (como en cualquier otro <i>cluster</i>) se garantiza mediante la relación de confianza mutua entre cada par de nodos en el <i>cluster</i> .
Red personal (<i>Personal Network</i>)	Una PN incluye la P-PAN y una colección dinámica de nodos y dispositivos personales remotos organizados en <i>clusters</i> , todos ellos conectados entre sí mediante infraestructura de interconexión.
Relación de confianza (<i>Trust Relationship</i>)	Dos partes que desean comunicarse entre sí constituyen una relación de confianza que determina el grado de certidumbre en la validez de las credenciales de cada uno para establecer un canal seguro de comunicación empleando mecanismos de cifrado. Esta relación se genera empleando los medios disponibles para el intercambio seguro entre los nodos.
Grabado o Marcado (<i>Imprinting</i>)	Procedimiento mediante el cual se inicializa la relación de confianza entre dos nodos. Básicamente consiste en un intercambio autenticado de claves.
Nodo personal (<i>Personal Node</i>)	Nodo vinculado a un usuario o persona con unos atributos de confianza preestablecidos. Este tipo de nodos es típicamente propiedad del usuario dueño de la PN. Sin embargo, cualquier nodo que incluya los atributos de confianza mutua necesarios para definir un <i>cluster</i> o grupo confiable de nodos puede ser considerado como un nodo personal. Estos atributos incluyen las claves criptográficas que, a no ser que sean canceladas, redefinidas o revocadas, permiten establecer dicha relación de confianza mutua.

Tabla 3.1: Terminología vinculada a las redes personales (continuación)

Nodo externo (<i>Foreign Node</i>)	Nodo no considerado como personal y que, por tanto, no puede formar parte de la PN. Los nodos externos pueden ser o no confiables. En el caso que sean de confianza, dicha relación con un nodo de la PN es efímera y se establece y mantiene para una acción específica.
Conectividad	
Coordinador radio	Entidad funcional lógica responsable de garantizar el acceso al medio dada una tecnología radio de comunicaciones.
Dominio radio	Conjunto de nodos o dispositivos que comparten una interfaz de comunicaciones sobre una misma tecnología radio gestionada por un único mecanismo de acceso MAC (centralizado o distribuido) y un único coordinador radio.
Red	
Nodo pasarela (<i>Gateway Node</i>)	Nodo personal dentro de un <i>cluster</i> que habilita la conectividad de los nodos y dispositivos de dicho <i>cluster</i> con el exterior.
Infraestructura de interconexión (<i>Interconnecting Structures</i>)	Redes públicas, privadas o compartidas, cableadas, inalámbricas o híbridas. Algunos ejemplos son una red móvil, Internet, una intranet o una red ad-hoc.
Servicio	
Servicio (<i>Service</i>)	Componente lógico implementado mediante un <i>software</i> que se ejecuta en un nodo y que ofrece una funcionalidad que una aplicación puede usar a través de una interfaz específica. Cada servicio dispone de una descripción formal que permite su descubrimiento. Dicha descripción debe incluir al menos información sobre qué ofrece el servicio, las interfaces de interacción y el nodo o equipo que lo ofrece.
Servicio personal (<i>Personal Service</i>)	Los servicios personales son aquellos provistos por nodos o dispositivos personales y disponibles únicamente para los nodos o dispositivos asociados a la PN. Esto implica que un servicio será accesible únicamente tras el establecimiento de una relación de confianza con el proveedor de dicho servicio.

Tabla 3.1: Terminología vinculada a las redes personales (continuación)

Servicio público (<i>Public Service</i>)	Los servicios públicos son aquellos servicios proporcionados por cualquier dispositivo o nodo tanto personal como externo. En este caso existirán servicios que sólo serán accesibles tras superar satisfactoriamente una etapa de autenticación/autorización (p. ej. servicios financieros, etc.) y otros que no la requieran y estén disponibles para cualquiera.
Contexto	
Contexto (<i>Context</i>)	Información que caracteriza a una persona, lugar u objeto. Se definen múltiples niveles de contexto: a nivel de usuario, red y entorno. La información de contexto se emplea, por ejemplo, en el descubrimiento inteligente de servicios.

La terminología descrita ayuda a introducir algunos de los conceptos de una PN. No obstante, para comprender mejor la relación existente entre las diferentes entidades, se incluye el diagrama *Unified Modelling Language* (UML) de la figura 3.2, en el que se representan los vínculos entre los términos definidos y la cardinalidad entre ellos.

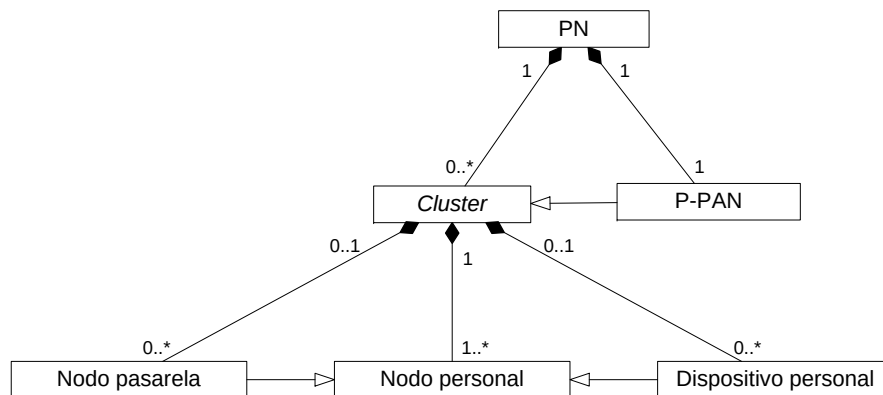


Figura 3.2: Relaciones entre las principales entidades de una PN

3.2. Visión general de la arquitectura de una PN

Las arquitecturas de red normalmente se describen considerando diferentes capas o niveles, cada uno de los cuales se sitúa sobre el anterior. En cada capa se agrupa un conjunto de funcionalidades de red interrelacionadas de forma que se reduzca la complejidad a la hora de hacer frente al sistema global. Esta división facilita el diseño modular independiente de forma que los cambios en una capa o nivel particular no supongan la actualización de la pila completa o de las capas adyacentes.

La arquitectura de red planteada para la PN se describe en la figura 3.3, que a su vez ofrece una comparativa con los modelos de red más conocidos. La arquitectura de la PN se asemeja a la de Internet considerando el modelo de referencia TCP/IP. La principal diferencia entre estos dos modelos reside en el nivel de enlace, que para el caso de la arquitectura de una PN se ha dividido en dos subcapas: una capa universal de convergencia (UCL, *Universal Convergence Layer*) y otra formada por múltiples capas de control de enlace de datos (DLC, *Data Link Control*). A continuación se descompone cada uno de los niveles en sus diferentes unidades funcionales y se profundiza en la descripción de cada uno de estos elementos.

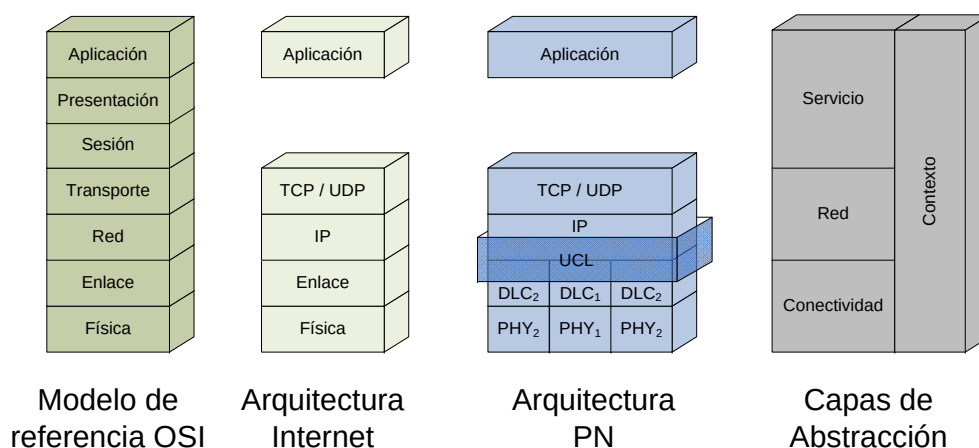


Figura 3.3: Comparativa de modelos de red

Dado que capas adyacentes de la arquitectura de red de una PN pueden compartir problemáticas similares, para facilitar la comprensión de la arquitectura planteada se ha decidido introducir una división más genérica en lo que se han denominado capas de abstracción. Esta nueva visión proporciona la posibilidad de analizar conjuntamente problemas en diferentes niveles, pero que están estrechamente ligados, y buscar la solución empleando entidades funcionales que operan en diferentes capas. Este mecanismo se conoce como optimización intercapas o *cross-layer optimization*.

En la figura 3.4 se muestran las cuatro capas de abstracción definidas. De abajo hacia arriba, el primer nivel de abstracción se denomina Capa de Abstracción a Nivel de Conectividad (*Connectivity Abstraction Level*). Esta capa engloba las capas 1 y 2 del modelo *Open Systems Interconnection* (OSI) y proporciona los mecanismos físicos necesarios para interconectar dispositivos heterogéneos. La Capa de Abstracción a nivel de Conectividad identifica, especifica e implementa las interfaces radio PAN necesarias para dar respuesta a los requerimientos del usuario dentro de su PN. El objetivo final del nivel de Conectividad es la provisión de los mecanismos necesarios para habilitar la comunicación segura entre los nodos y dispositivos heterogéneos que conforman la PN.

La Capa de Abstracción a Nivel de Red (*Network Abstraction Level*) se sitúa justo por encima de la de Conectividad. En ella se hace frente a los problemas inherentes de las capas de red y transporte, niveles 3 y 4 del modelo OSI. Asimismo, sirve de apoyo al nivel de enlace dando cabida a las necesidades de redirección o retransmisión de información. Los

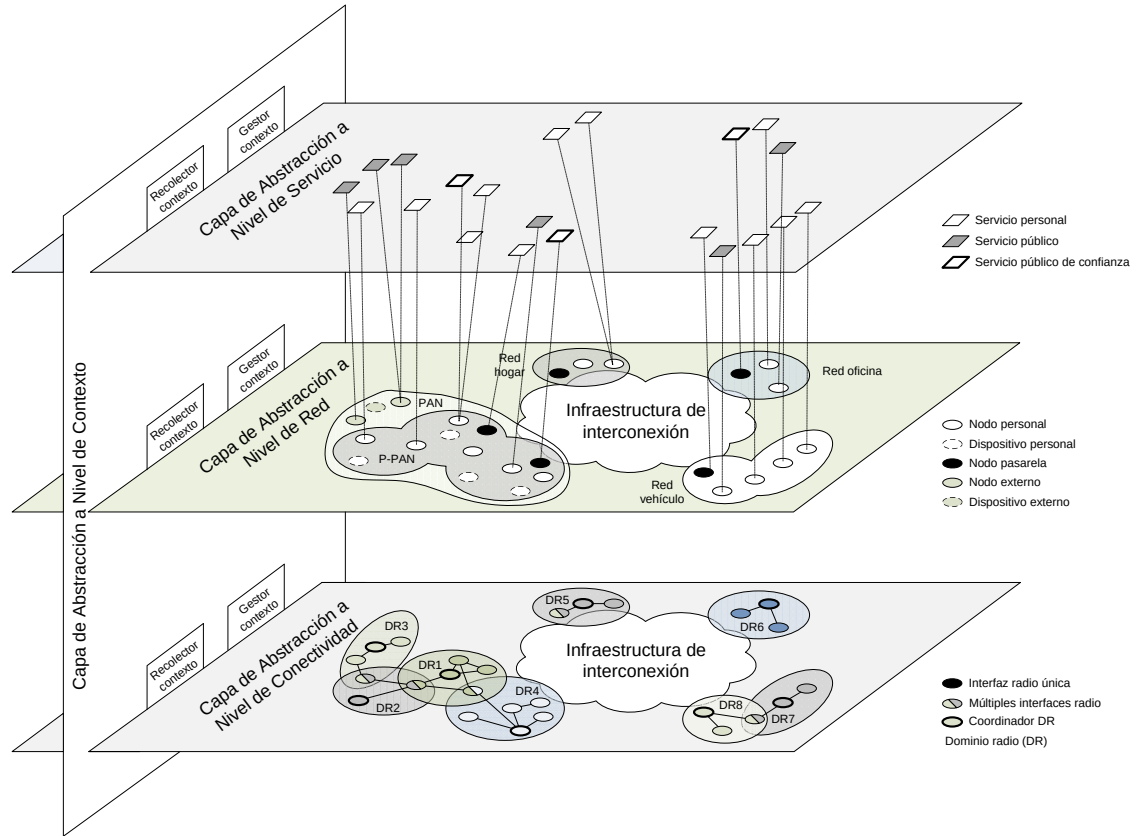


Figura 3.4: Visión de una PN en capas de abstracción

conceptos de *cluster* y, más específicamente, el de P-PAN, comienzan a tener sentido en esta capa. El concepto de PN, como extensión de la P-PAN y definido como la agregación de todos los nodos personales activos, tanto remotos como en las proximidades del usuario, también es ahora cuando empieza a cobrar sentido.

En lo más alto y cercano al usuario, se encuentra la denominada Capa de Abstracción a Nivel de Aplicación o Servicio (*Service Abstraction Level*). Los servicios son, en la práctica, la interfaz con el usuario. En este nivel se abordan las cuestiones relacionadas con la creación, publicación, descubrimiento y uso de servicios tanto dentro como fuera de la PN. El descubrimiento y la provisión de servicios son aspectos importantes dentro de la arquitectura de la PN dado que sin el despliegue de procedimientos inteligentes de descubrimiento y provisión el usuario no verá su PN como una red, sino como un conjunto aislado de nodos que proporcionan servicios de manera individual pero siguiendo unas normas de seguridad. Es, por tanto, la Capa de Abstracción a Nivel de Servicio la que unifica la gestión del uso de servicios en el ámbito de la P-PAN/PN.

Adicionalmente, se añade una cuarta capa transversal a las otras tres. Esta capa, Capa de Abstracción a Nivel de Contexto (*Context Abstraction Level*), incluye todo lo relacionado con la adquisición y gestión del contexto tanto del usuario, como de los nodos y dispositivos, como de la PN como entidad. La información de contexto se encuentra disponible en todas las capas, por lo que los diferentes componentes o entidades funcionales operando en esta

capa deben ser capaces de interaccionar con el resto de las capas. No obstante, aunque la adquisición es un proceso distribuido, es recomendable que la gestión de la información se realice de forma centralizada y global. Gracias a la labor realizada en esta capa, a partir de múltiples y heterogéneas fuentes de información de contexto se derivan datos o estadísticas relevantes que serán compartidas con los componentes de las diferentes capas de la pila de comunicaciones y servirán como base para la toma de decisiones que afecten a su operativa.

Antes de profundizar en la descripción de las particularidades de cada nivel de abstracción, es necesario introducir los conceptos básicos de seguridad dentro de la PN. Aunque la seguridad no se ha reflejado como una capa de abstracción en sí misma, es, como se ha podido comprobar hasta el momento, uno de los puntos destacables en la arquitectura y funcionamiento de una PN. En este sentido, la seguridad está incluida en todas y cada una de las capas y se basa en los conceptos de relación de confianza a corto y largo plazo. La confianza a largo plazo, que puede ser considerada como permanente, se emplea para establecer una asociación o vínculo fuerte entre nodos y dispositivos de la PN, pudiéndose extender excepcionalmente a otros nodos. Para instaurar la confianza entre los componentes de la PN, especialmente entre aquellos que forman parte de la P-PAN, se hace uso de procedimientos criptográficos que se sustentan en un secreto compartido entre los nodos, consistente en este caso en un conjunto de claves criptográficas. De esta forma se facilita la formación segura de la P-PAN y la PN, así como la provisión segura de servicios. Por su parte, la confianza a corto plazo tiene una duración temporal preestablecida, que puede ser una sesión o un tiempo fijo, y sirve como base para garantizar el intercambio seguro de información. En el capítulo 4 se ahondará más en estos y otros aspectos de la seguridad en las redes personales.

En las siguientes secciones se detalla cada una de las subcapas, aprovechando la ocasión para describir las entidades y los procedimientos involucrados en la creación y mantenimiento de una PN.

3.3. Capa de Abstracción a Nivel de Conectividad

La Capa de Abstracción a Nivel de Conectividad es la capa de nivel inferior dentro de la representación de la arquitectura de una PN en capas de abstracción. Para un mejor seguimiento de las explicaciones, en la figura 3.5 se incluye el diagrama de esta capa de abstracción.

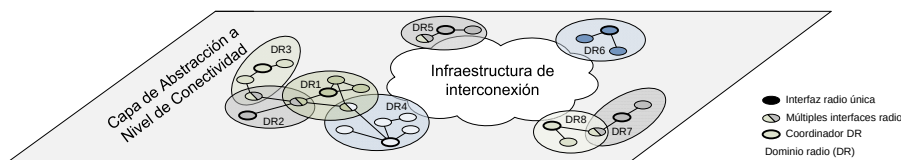


Figura 3.5: Capa de Abstracción a Nivel de Conectividad

En este nivel, los dispositivos y nodos se organizan en dominios radio (DR). Un DR describe el área en el que los dispositivos, con independencia de su dueño, pueden comunicarse entre ellos a nivel MAC usando un canal de control MAC común. Este canal de control se emplea, entre otras cosas, para evaluar de manera distribuida o coordinada si el canal de

comunicaciones se puede emplear para intercambiar información entre dos o más dispositivos. Entre las tecnologías radio a incorporar en los nodos o dispositivos de una PAN se encuentran todas aquellas estandarizadas y de uso común, como IEEE 802.11, Bluetooth, IEEE 802.15.x, etc.

Dado que los orígenes de las PN están vinculados al proyecto MAGNET, a las tecnologías enumeradas hay que añadir la propia tecnología de comunicaciones radio diseñada y desarrollada durante este proyecto. Esta nueva tecnología nace con el objetivo de ofrecer un mejor rendimiento bajo las premisas de la PN y soporta tanto el modo de operación LDR como HDR. El modo LDR presenta unos requerimientos estrictos en cuanto a coste y consumo de energía, lo que hace que sea prácticamente inviable el desarrollo de una interfaz radio escalable barata y energéticamente eficiente al tiempo que permita el acceso a servicios multimedia HDR. Consecuentemente, la interfaz radio MAGNET plantea un procedimiento similar al seguido por IEEE [80, 81] desarrollando dos versiones diferentes de tecnologías de comunicaciones radio, cada una ajustada a los requerimientos particulares de cada modo de operación. Resulta, por tanto, que la versión LDR de MAGNET limita su rango de aplicación a sensores y actuadores, tales como sensores corporales móviles (de aplicación en BAN), es decir, dispositivos de una complejidad muy reducida. Por su parte, la versión HDR se enfoca a su empleo en nodos más potentes, tales como teléfonos móviles inteligentes (*smartphones*), *Personal Digital Assistants* (PDA), tabletas, etc., que requieran capacidades de comunicación de corto alcance para soportar servicios multimedia.

La gestión de cada DR se plantea como una tarea centralizada, siendo asignado el rol de coordinador a un único nodo del DR. Con un canal de comunicaciones radio gestionado de forma centralizada se busca minimizar las interferencias y optimizar potencia transmitida; como resultado, se ofrece al usuario de la PN la mejor opción en términos de calidad del enlace según las condiciones del entorno. Dado que las tecnologías radio existentes no son sensibles ni conscientes del contexto por sí mismas, la especificación del interfaz radio MAGNET se centra principalmente en ofrecer estas características sobre el nivel físico.

En esta tesis no se pretende dar un mayor nivel de detalle sobre el diseño e implementación de las soluciones que soporten una PN a nivel físico, por lo que se recomienda a todo aquel lector que esté interesado acudir a [82-87], entre otros, para profundizar en la especificación de la interfaz radio MAGNET. No obstante, el *software* de control de dicha interfaz (*drivers*, etc.) que permite la integración dentro de la pila de comunicaciones sí se ha realizado como parte del trabajo en esta tesis, quedando el detalle del diseño y desarrollo reflejado en [88].

Es innegable que a la vista de las capacidades previstas para las PN resulta virtualmente imposible dotarlas todas mediante una única tecnología inalámbrica, un único DR y un único modelo de dispositivo. Es por esto que entre las características de la Capa de Abstracción a Nivel de Conectividad se ha destacado la heterogeneidad no sólo de dispositivos y nodos de usuario, sino también de tecnologías inalámbricas. En los escenarios como el planteado en la figura 3.6, pueden coexistir en cada dispositivo múltiples interfaces con tecnologías inalámbricas diferentes, teniendo cada una su entorno de aplicación; unas serán más adecuadas para comunicaciones de corto alcance a altas velocidades, mientras que otras serán más apropiadas para realizar la interconexión con la infraestructura. Por lo tanto, dado que cualquier nodo puede estar equipado con varios interfaces de red de diferentes tecnologías, ese nodo podrá pertenecer a más de un DR. Por otro lado, debido a que cada tecnología

radio es particular, no podrán interoperar entre ellas de forma directa. Aplicando uno de los principales requerimientos de la PN que estipula que ésta debe ser altamente segura al tiempo que amigable para el usuario, se hace indispensable el diseño de una solución que soporte y a la vez oculte al usuario la complejidad inherente resultante de la existencia y uso de múltiples tecnologías de comunicación.

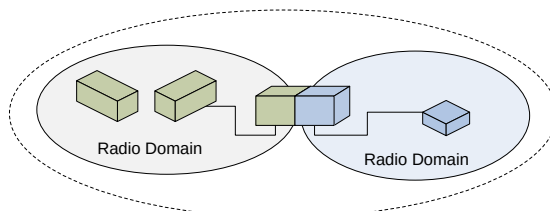


Figura 3.6: Ejemplo de nodo operando en múltiples dominios radio

Se comprueba, pues, que hacer realidad las PN es un reto que requiere la integración de muchos subsistemas, cada uno de los cuales trata de dar respuesta a necesidades específicas impuestas por el concepto de PN [89]. La Capa de Abstracción a Nivel de Red se centra principalmente en las comunicaciones dentro del *cluster* (intra-*cluster*) en modo ad-hoc y la conexión de los *clusters* (inter-*cluster*), usualmente a través de una infraestructura común. La solución para muchas de las problemáticas descritas a nivel de conectividad, entre las que destacan el soporte a la heterogeneidad de interfaces radio, la seguridad, etc. aparentemente no se encuentra a nivel de red, si bien la colaboración entre ambas capas, conectividad y red, podría ayudar considerablemente. De ahí que en la PN se defina una nueva entidad o subcapa intermedia, denominada UCL, que servirá de nexo y ayudará a abordar todas esas problemáticas pendientes de resolver. La UCL permite gestionar de forma conjunta todas las interfaces de diferentes tecnologías inalámbricas residentes en un mismo nodo o dispositivo. Esta característica la habilita para dar respuesta a la necesidad de soporte de comunicaciones a través de múltiples interfaces, a la selección óptima de la estrategia de selección y uso de la red, a la operativa de comunicaciones eficiente energéticamente y a la protección de las comunicaciones. Destacar además que la UCL hace uso del paradigma de optimización intercapas, gracias a lo cual es capaz de obtener y tratar datos provenientes de múltiples fuentes al tiempo que actúa sobre dichas fuentes sustentándose en las decisiones basadas en el contexto analizado. La aplicación del paradigma de optimización intercapas hace de la UCL el nexo de unión de las diferentes capas de abstracción. En la siguiente sección se describe en detalle la UCL.

3.4. Capa Universal de Convergencia

Los nodos y dispositivos de una red personal presentan una gran heterogeneidad en términos de capacidades de comunicaciones, pudiendo llegar a integrar varias interfaces radio en un mismo terminal. La gestión inteligente y transparente para el usuario supone un reto al que las PN deben hacer frente. En este sentido, la idea de desacoplar las capas superiores de las tecnologías inalámbricas subyacentes y dar soporte real a comunicaciones multimodales se puede lograr haciendo uso de lo que en una PN se ha denominado UCL.

3.4.1. Principios de diseño

Esta nueva capa se sitúa en una zona intermedia entre la Capa de Abstracción a Nivel de Conectividad y la Capa de Abstracción a Nivel de Red. Su emplazamiento privilegiado en la pila de comunicaciones permite a la UCL abordar las comunicaciones inteligentes desde dos puntos de vista. Por un lado, la definición de una interfaz de intercambio con la capa de red común para todas las tecnologías de acceso radio (RAT, *Radio Access Technology*), que gestiona dichas interfaces independientemente de sus capas físicas y MAC, permite dotar a la pila de comunicaciones de compatibilidad tanto con las tecnologías existentes como con las futuras. Por otro lado, la UCL también emplea el paradigma de optimización intercapas, consistente en violar la norma que prohíbe la comunicación directa y el intercambio de información entre capas no adyacentes de la pila de comunicaciones. Así, gracias a su localización, la UCL dispone de la capacidad de poder analizar tanto flujo de información entrante o ascendente y, por ejemplo, usar la información de la relación señal a ruido (SNR, *Signal-to-Noise Ratio*) para enriquecer el proceso de toma de decisiones en el algoritmo de encaminamiento ad-hoc, como el saliente o descendiente para afinar los valores de los parámetros de MAC en función del estado de la batería o los requerimientos de QoS. En el apartado 3.7 se profundizará en la descripción de la recogida de métricas en las diferentes capas de abstracción y la vinculación del contexto de la PN con las soluciones de optimización intercapas.

Antes de proceder con la descripción de la arquitectura, se analizan las características principales que la UCL debe ofrecer, que serán la base para el diseño de una solución que se ajuste a las necesidades de la PN.

3.4.1.1. Abstracción del nivel de enlace

Uno de los principios más relevantes seguido en el diseño de la UCL es el acceso uniforme y transparente a las diversas características intrínsecas de las tecnologías de red que incorpore el terminal empleado por el usuario. Este principio se ha empleado con éxito en propuestas anteriores como [90-93], donde se describen arquitecturas de nivel de enlace que permiten comparar y evaluar diferentes tecnologías de acceso heterogéneo en base a capacidades y rendimientos del nivel de enlace con el fin de asignar los recursos de red adecuados que cumplan con los requerimientos del servicio. Sin embargo, vale la pena recalcar que la UCL va más allá, teniendo en cuenta no sólo la información del nivel de acceso radio a la hora de elegir la mejor interfaz, sino también otras fuentes de información como el perfil y las preferencias del usuario u otra información de contexto.

3.4.1.2. Entidad cognitiva

Otro de los principios de diseño es la utilización de algoritmos de decisión multi-paramétricos que permiten elegir la mejor interfaz de comunicaciones en función de la información recibida de diversas fuentes, actuando en consecuencia sobre los flujos de información de acuerdo a esas decisiones.

La gran diversidad de información a tener en cuenta durante el proceso de decisión, unida a la necesidad de usar algoritmos que requieran la menor carga computacional posible (debido al hecho de tener que ser implementados en terminales con ciertas restricciones)

hace que la UCL posiblemente tenga que utilizar técnicas de decisión del tipo *Multi-Attribute Decision Making* (MADM) de manera similar a como se han utilizado en [94-96]. Muchas de esas técnicas emplean variables que permiten dar el peso adecuado a cada parámetro en función de su relevancia durante el proceso de toma de decisiones. La elección del peso correcto de cada variable permite obtener finalmente la decisión más adecuada. En este sentido, es necesario recurrir a técnicas de optimización [97] que permiten encontrar el límite superior del rendimiento del algoritmo empleado. Y todo ello, en el caso ideal, deberá ser realizado en tiempo real de forma que las decisiones se adapten de la forma más rápida al contexto dinámico que rodea al usuario y a sus terminales.

3.4.1.3. Independencia de los servicios

Los servicios tradicionales, aquéllos más comunes y con mayor grado de implantación como por ejemplo navegadores web, clientes de voz sobre IP (VoIP, *Voice over IP*), etc., no tienen conocimiento de la UCL, y en el caso de que no sean desarrollados expresamente por el usuario, tampoco lo tendrán de su ejecución dentro de un entorno tan singular como la PN. Con el fin de no excluir a estos servicios de las ventajas que la UCL, en particular, y la PN, en general, ofrecen, se plantea como principio de diseño que la UCL opere independientemente del servicio o aplicación que necesite hacer uso de las capacidades de comunicación del dispositivo. Por tanto, debe ofrecer interfaces genéricas.

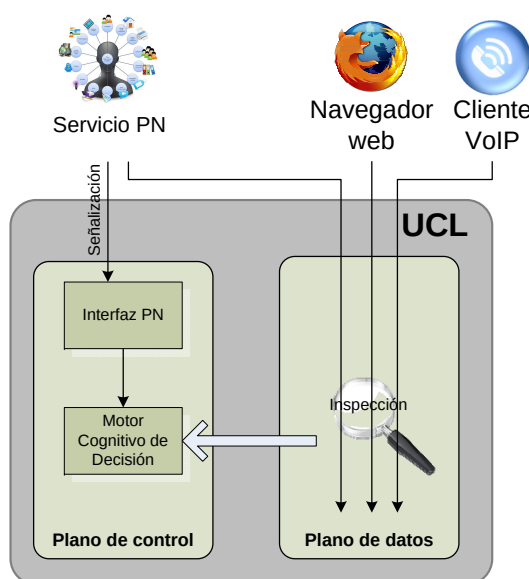


Figura 3.7: Visión de planos de control y datos de la UCL

En este sentido, la funcionalidad de la UCL deberá estar embebida en la propia pila de protocolos extrayendo y realizando las operaciones necesarias sobre los flujos de datos para mejorar el rendimiento, la seguridad, la calidad de servicio y la experiencia del usuario. En la figura 3.7, se muestra, a modo de ejemplo, el impacto que tiene este principio de diseño en el flujo de datos y de control de algunas aplicaciones tradicionales y de los servicios enfocados a la PN. Todo el flujo de la información (datos y control) de los servicios tradicionales pasará

únicamente a través del plano de datos, mientras que los otros podrán, al ser conscientes de la existencia de la UCL, interactuar con ella a través de su plano de control.

3.4.1.4. Proveedor de contexto

Teniendo en cuenta el principio anterior por el cual la UCL tendrá acceso a una amplia gama de parámetros relacionados con las interfaces de red subyacentes, la UCL se erige como un elemento proveedor de contexto del entorno de comunicaciones del usuario y deberá implementar los mecanismos necesarios para realizar intercambios fluidos con las entidades funcionales que operen en la Capa de Abstracción a Nivel de Contexto.

3.4.2. Descripción general

La UCL se despliega como una capa de DLC superpuesta sobre las capas de DLC particulares de las diferentes tecnologías de acceso, pero sin modificar la operativa de éstas. Así, la UCL puede añadirse dentro de la pila de protocolos de forma transparente sin que las capas superiores ni las inferiores se vean afectadas. Merece la pena hacer hincapié en el hecho de que la UCL permite no sólo la comunicación entre nodos que incluyen la UCL en su pila, sino también con todos aquellos que tiene una pila de comunicaciones TCP/IP estándar. Ello supone una gran ventaja con respecto a otras soluciones [93, 98-100], que únicamente permiten la comunicación entre iguales.

La figura 3.8 presenta un esquema con los principales componentes funcionales que puede incluir la UCL, donde se observa una estructura modular en la que cada uno de los módulos se especializa en realizar una tarea que se desea que la UCL ofrezca. Este diseño modular, que se describe seguidamente, hace que sea sencillo incorporar o eliminar funcionalidades y adaptar el comportamiento a las características y requerimientos del sistema sobre el que la UCL correrá.

3.4.2.1. Capa de adaptación

Uno de los principales objetivos de la UCL es hacer lo más transparente y sencilla posible la gestión de las múltiples interfaces inalámbricas disponibles. En este sentido la solución más adecuada consiste en aglutinar todas las interfaces bajo una única interfaz de red virtual, de forma que las capas superiores tengan un solo punto de acceso a la red. Mientras que el plano de control se encarga de extraer información relevante sobre las diferentes tecnologías de acceso disponibles y los mecanismos nativos que incorporan para la gestión de los flujos de datos, el plano de datos actúa de manera transparente sobre los paquetes de forma que las comunicaciones se realicen de la manera más adecuada en cada momento (p. ej. emplear la RAT de transmisión óptima bajo un determinado parámetro).

La versatilidad de la UCL permite otros modos de operación en los que cada una de las interfaces de red existentes mantiene su propia identidad. En esta configuración la UCL actúa únicamente como una capa de coordinación y gestión de las interfaces subyacentes, siendo éstas visibles al usuario.

La opción preferente para desplegar en la PN es la que exporta una interfaz virtual, pues oculta completamente al usuario toda la complejidad existente en términos de comunicaciones.

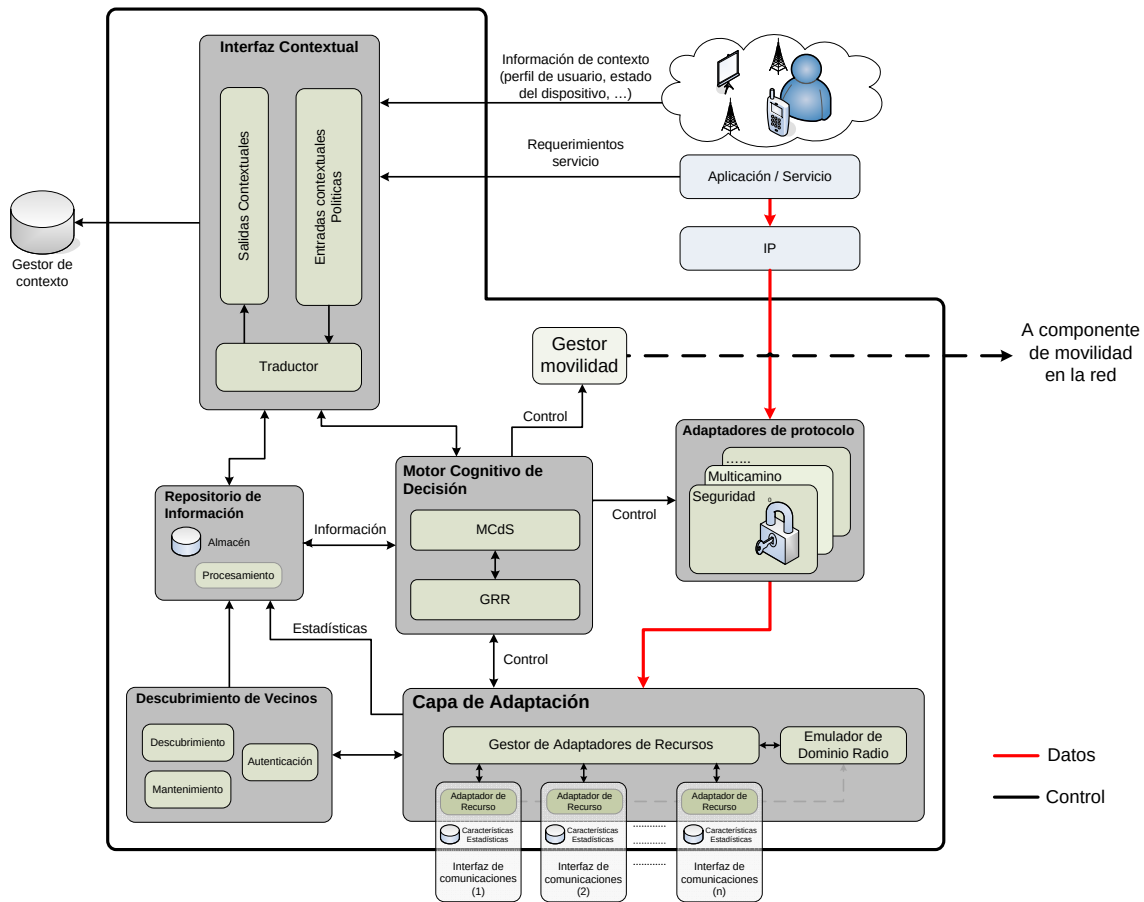


Figura 3.8: Arquitectura de alto nivel de la UCL

Los componentes que forman la Capa de Adaptación (CdA) son los Adaptadores de Recursos Radio (ARR) y el Gestor de Adaptadores de Recursos (GAR), en el que cobra especial relevancia el Emulador de Dominio Radio (EDR). Todos ellos se describen a continuación.

3.4.2.1.1. Adaptadores de recursos radio

Se trata de módulos específicos que interactúan con cada una de las interfaces de comunicaciones. Son los encargados de transformar los comandos genéricos en implementaciones específicas de la interfaz correspondiente. Asimismo, son los encargados de extraer las estadísticas de cada interfaz.

3.4.2.1.2. Gestor de adaptadores de recursos

El GAR se encarga de coordinar los distintos ARR. Exporta las estadísticas a través de una interfaz única, ofrece una serie de comandos genéricos mediante los cuales se puede actuar sobre el proceso de envío y recepción de tráfico, y gestiona los diferentes flujos de datos orientándolos hacia la interfaz de salida oportuna.

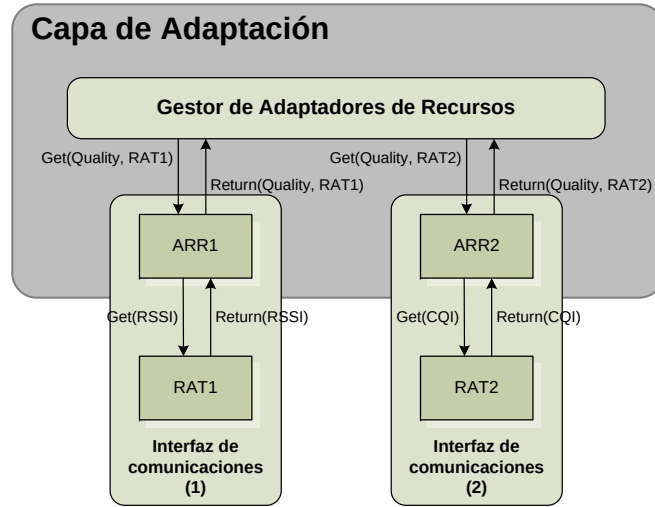


Figura 3.9: Interacciones en la Capa de Adaptación

La figura 3.9 muestra un ejemplo que revela la importancia de las funcionalidades de la CdA en la normalización y gestión de las estadísticas. Supóngase un terminal con dos interfaces radio diferentes: una monitoriza su calidad de señal en base al valor del *Received Signal Strength Indication* (RSSI) y la otra en base al *Channel Quality Indicator* (CQI). Cuando el GAR precise obtener el valor de calidad de la señal de una interfaz radio, enviará un comando genérico al ARR correspondiente utilizando la *Application Programming Interface* (API) proporcionada por éste, por ejemplo `Get(Quality, RATx)`. El ARR recibe dicho comando y, al tener pleno conocimiento de las características intrínsecas de su interfaz, utiliza el comando específico para obtener la información solicitada, por ejemplo `Get(RSSI)`.

Adicionalmente, la gestión del funcionamiento de las interfaces radio subyacentes se apoya en las instrucciones derivadas de la aplicación de algoritmos cognitivos de decisión sobre las métricas recogidas y atendiendo al contexto y preferencias del usuario. El GAR ejecutará los comandos necesarios para que se apliquen dichas instrucciones.

3.4.2.1.3. Emulador de dominio radio

Por definición de DR, todos los nodos dentro de un mismo DR pueden comunicarse entre sí sin tener que hacer uso de facilidades de encaminamiento a nivel de red. Sin embargo algunas tecnologías, como por ejemplo Bluetooth, no soportan este modo de funcionamiento dado que siguen un modo de operación orientado a la conexión que implica la obligatoriedad de establecer una conexión punto a punto con un nodo central. En este caso, todas las comunicaciones están centralizadas en un nodo formando una topología en estrella. Gracias al módulo de gestión de interfaces radio, la UCL se encarga de distribuir los paquetes recibidos al resto de los nodos en el DR, logrando así emular el comportamiento de un DR.

Llegados a este punto es importante señalar que a la hora de definir cómo establecer las comunicaciones entre diferentes DR se barajan principalmente dos alternativas: una de ellas implica que las comunicaciones ad-hoc se realizan a nivel de enlace, mientras que la

otra se apoya en soluciones a nivel de red. Como es natural, ambas tienen sus ventajas e inconvenientes; la primera libera a la capa de red de todas las tareas de gestión de encaminamiento multisalto al tiempo que hace realidad el concepto de DR. Adicionalmente, dado que la redirección de tramas se realiza a nivel de enlace, mediante puentes de red o *bridges*, la velocidad de transferencia se incrementa al tener que recorrer la información un menor número de capas de red. La aplicación de esta solución supone la definición de protocolos multisalto a nivel de enlace (*multi-hop ad-hoc bridging protocols*) de forma que se permita la interconexión entre nodos de diferentes DR o nodos dentro del mismo DR pero no en el radio de cobertura (ver figura 3.5).

La segunda aproximación consiste en hacer uso de la solución normalmente empleada para resolver la problemática de las comunicaciones multisalto a nivel de red. Ha sido estudiada en profundidad dentro de MANET [30-33, 74]. Considerando la opción de una UCL que defina un único identificador de red compartido por todas las interfaces bajo su paraguas, la gestión de encaminamiento multisalto en un entorno inalámbrico heterogéneo no reporta ninguna necesidad adicional.

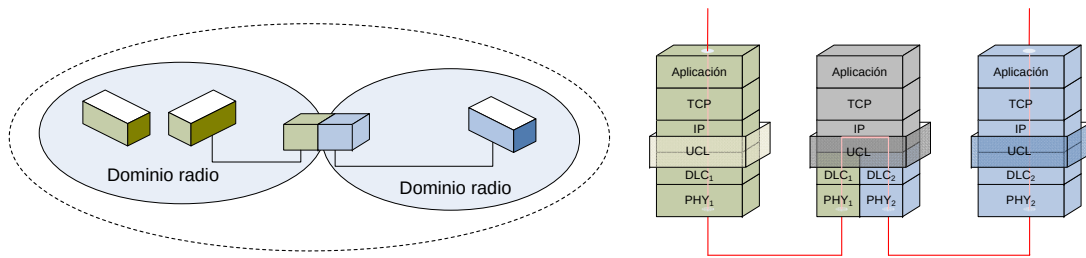


Figura 3.10: Gestión multiradio en la UCL

Tras valorar ambas opciones y buscando la generalidad de la solución, la decisión tomada fue la de no habilitar el soporte para comunicaciones inter-DR a nivel de enlace y hacerlo usando los protocolos de encaminamiento ad-hoc. La figura 3.10 muestra una visión general del procedimiento para llevar a cabo el intercambio de información entre nodos con múltiples interfaces radio.

3.4.2.2. Motor cognitivo de decisión

El Motor Cognitivo de Decisión (MCD) se puede considerar como la entidad que dota de inteligencia a la UCL, pues es el encargado de definir cómo adaptar el comportamiento de las comunicaciones a las necesidades de la PN. El MCD está dividido en dos módulos que se reparten la jerarquía de decisión. En este sentido, las decisiones sobre qué requisitos necesitan ser considerados como candidatos potenciales a la hora de asignar recursos a los servicios, se toman en el Módulo de Calidad de Servicio (MCdS), que es el encargado de maximizar la experiencia del usuario. Por otro lado, los mecanismos que deciden la forma de asignar esos recursos haciendo el mejor uso de las capacidades subyacentes se implementan en el Gestor de Recursos Radio (GRR). La figura 3.11 muestra la relación entre los módulos del MCD, cuyas características se describen a continuación.

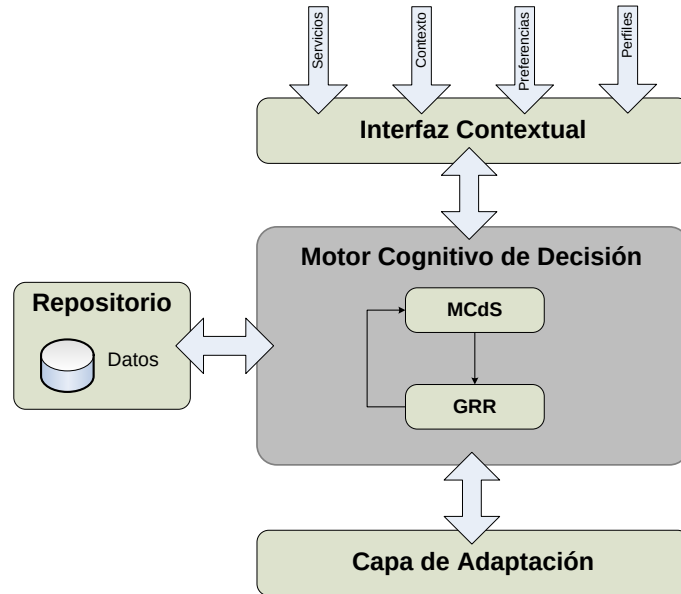


Figura 3.11: Interacciones en el Motor Cognitivo de Decisión

3.4.2.2.1. Módulo de calidad de servicio

Este módulo es el encargado de la toma de decisiones basadas en las diferentes entradas provenientes de los servicios, gestor de contexto, preferencias, perfiles de usuario, métricas de los recursos radio, etc. El MCdS procesa toda esta información y selecciona el subconjunto de requisitos, que a través del GRR, se aplicarán sobre los interfaces de red.

El MCdS desconoce las características de todas las interfaces de comunicación y, por tanto, realiza el procesamiento basándose en la información de uso actualizada que el GRR le proporcione. Además empleará todos los datos disponibles tanto en el repositorio local de información como los adquiridos a través de los interfaces contextuales. Por otra parte, y gracias a mecanismos de inferencia y aprendizaje, el MCdS será capaz de adaptar sus decisiones dinámicamente.

Si es necesario, el MCdS activará los Adaptadores de Protocolo (AdP) necesarios para cumplir con los requisitos que no han sido seleccionados. Este puede ser el caso de un entorno de comunicaciones poco seguro que no cumpla con las premisas impuestas por la PN. Existirá, por tanto, un AdP que actuará sobre el paquete de información para garantizar la transmisión segura de los datos.

3.4.2.2.2. Gestor de recursos radio

Es el encargado de asignar y coordinar los recursos de comunicación de los que dispone el terminal móvil en función de las especificaciones de QoS definidas en el MCdS y del conocimiento que posee acerca de las capacidades del terminal. Para ello, obtiene toda la información acerca de los recursos radio del terminal a través de la CdA, selecciona la interfaz o grupos de interfaces de red más óptimos, y asigna los recursos radio que son necesarios. Esto permite al GRR dar un tratamiento individualizado a cada flujo de datos,

asignando de manera óptima los recursos que, en la medida de lo posible, cumplan los requisitos exigidos.

3.4.2.3. Descubrimiento de vecinos

Es necesario tener conocimiento de los nodos cercanos si se quiere definir un *cluster* y sus límites. Sin embargo, no todas las RAT disponen de mecanismos para poder proporcionar la identidad y capacidades de los nodos más cercanos. El módulo de Descubrimiento de Vecinos define las funcionalidades para hacer frente a esta necesidad. Se opta por definir la operativa de este módulo en modo proactivo, priorizando la inmediatez en el reconocimiento de recursos sobre el consumo energético.

La búsqueda de nodos y dispositivos se realiza en el nivel de conectividad, donde cualquier equipo tiene a su alcance a todos aquellos que se encuentran en su mismo DR a un salto de distancia. Para informar de su presencia, los nodos difunden de manera periódica mensajes de anuncio (*beacons*). El período entre *beacons* consecutivos se escoge para que se adapte a la dinamicidad de la red; es decir, para redes donde se prevé que la movilidad de los nodos o los cambios de estado sean reducidos, se establecerá un período largo, mientras que en redes muy variables este valor será pequeño. La elección óptima de dicho período deberá realizarse buscando un compromiso entre la potencia consumida y la velocidad en las actualizaciones que se desee. Será un valor muy dependiente del contexto del *cluster*.

Por otro lado, cabe recordar que los nodos que forman parte de la PN mantienen una relación de confianza mutua entre ellos, iniciada con la supervisión del usuario tras llevar a cabo el proceso de marcado del nodo (*imprinting*). La formación segura del *cluster* se basa en claves bilaterales compartidas entre dos nodos con una larga validez temporal, que reflejan la relación de confianza existente entre dichos nodos. Por tanto, el procedimiento de descubrimiento de vecinos no sólo debe identificar a los nodos en las proximidades, sino también determinar cuáles son o no de confianza con el fin de poder establecer un canal de comunicaciones seguro. En este sentido, en el diseño de este módulo se han identificado varios niveles de confianza dado que no todos los nodos tienen por qué pertenecer a la misma PN:

- Externo (*Foreign*): nodo cuya participación en la PN no ha sido aún verificada. Por consiguiente, se asume que se trata de un nodo no confiable y solo se permite una comunicación pública con él.
- Personal: nodo que pertenece a la PN. Ha superado el procedimiento de autenticación satisfactoriamente y su identidad ha sido verificada. Todo nodo personal se considera un nodo externo hasta que se comprueba que pertenece a la PN.
- Amigo (*Friend*): tipo especial de nodo con el que se ha establecido una relación de confianza temporal o a corto plazo. La identidad de dicho nodo se ha comprobado durante la fase de descubrimiento. La compartición de servicios y recursos no es total, pero se puede considerar como la base de lo que en el capítulo 5 se describe como PN-F.

La lista de nodos vecinos se almacena en una base datos interna, donde se mantiene la referencia al tipo de relación existente entre el nodo local y cada uno de sus vecinos. Haciendo

uso de las capacidades de interacción multi-capa de la UCL, toda esta información se puede exportar al protocolo de encaminamiento multisalto, evitando así la duplicación de mensajes de descubrimiento y/o de difusión de identidad [101]. La ventaja de este mecanismo es que además de informar de la identidad del nodo y su estado en la red se adjunta información sobre la relación de confianza con él, lo que permite optimizar las rutas generadas, permitiendo redirigir tráfico personal sólo a través de nodos personales o de confianza.

3.4.2.4. Repositorio de información

La intención de hacer de la UCL una capa que permita la implementación del paradigma de optimización intercapas y dotarla de la inteligencia suficiente para tomar decisiones de comunicaciones, hace que sea necesario la inclusión de una entidad funcional capaz de gestionar la información y hacerla accesible a aquellos que la requieran. Si el MCD se considera la inteligencia de la UCL, el repositorio de información es la memoria del mismo.

La UCL aloja en su repositorio conocimiento en diferentes áreas, obtenido a partir de las múltiples interfaces externas que posee. A nivel de enlace y físico dispone de datos sobre los nodos vecinos, la calidad del enlace, el grado de utilización de una interfaz de red determinada y el ancho de banda libre, etc. De nivel de red y superiores, aloja métricas relativas a los flujos de datos que se originan o reciben, como identidad de los extremos, seguridad aplicada, protocolos más empleados, etc.

Estos y otros datos que se puedan obtener del entorno de gestión de contexto de la PN, serán las variables que adapten los algoritmos y procedimientos ejecutados en el MCD.

3.4.2.5. Interfaz contextual

Gran parte de la información que la UCL necesita para gestionar de manera inteligente los flujos de comunicaciones de datos, la recolecta por sí misma a través de los módulos de análisis y gestión de las comunicaciones. No obstante, las necesidades y requisitos impuestos por el usuario, por la propia infraestructura que la rodea en un momento dado o por los servicios a los que corresponden esos flujos son adquiridos a través de la interfaz contextual.

Esta interfaz no tiene por qué ser unidireccional, sino que la propia UCL se puede convertir en un proveedor de información relevante para otras entidades. La inclusión de este módulo dentro de la arquitectura de la UCL permite al entorno de gestión de contexto tener acceso a información actualizada del sistema de comunicaciones [102]. La información recolectada se exportará al sistema de gestión y distribución de contexto, haciendo que la información local esté disponible para otros nodos de la PN. Así se tendrá una visión más completa de la situación de la PN.

3.4.2.6. Adaptadores de protocolo

Se ha insistido en la idea de la UCL como un gestor inteligente de las comunicaciones. En numerosas ocasiones, las decisiones que tome suponen modificaciones en el flujo de datos, llegando incluso a modificar los propios datos que se transmiten. Los AdP, operando dentro del plano de datos, se encargan de aquellas funcionalidades o procedimientos que deban ser de aplicación para soportar los requerimientos impuestos bien por el usuario, por los

servicios o por la propia UCL a través del MCD, y que no sean soportadas de manera nativa en las tecnologías de red disponibles.

Siempre que sea posible, se intentará emplear el soporte nativo que ofrezca la interfaz de red para una funcionalidad solicitada por el MCD, pero en caso de que no estuviera disponible y un AdP lo implementase, el MCD lo activará para cumplir con los requerimientos impuestos. Algunos ejemplos pueden ser seguridad (cifrado y autenticación), compresión de datos, corrección de errores, optimización de rutas, etc.

3.4.2.6.1. Seguridad

El caso de la PN es un caso singular en la gestión de las comunicaciones, especialmente en lo concerniente a la seguridad. La singularidad de los procedimientos definidos para cifrar y autenticar las conexiones entre nodos personales, ideada para sobreponerse a las deficiencias de seguridad existentes en la mayoría de las tecnologías inalámbricas, hace prácticamente obligatoria la incorporación de un AdP centrado en la seguridad. Este AdP opera en colaboración con el módulo de descubrimiento de vecinos, empleando las claves bilaterales derivadas.

La mayoría de los trabajos realizados en comunicaciones multisalto se ha concentrado en algoritmos de encaminamiento *unicast*, y a raíz de ello se han especificado varios protocolos en la IETF. No obstante, los protocolos de encaminamiento MANET más actuales [103, 104] confían implícitamente en los nodos de la red empleados en la ruta para llegar al destino. La ingenuidad de este modelo permite a nodos maliciosos poder llegar a paralizar una red ad-hoc añadiendo actualizaciones de rutas incorrectas, enviando mensajes de encaminamiento erróneos, etc.

El AdP orientado a la seguridad da respuesta a uno de los mayores retos planteados en la P-PAN y en cualquier otro de los *clusters* de la PN, esto es, lograr la seguridad extremo a extremo en el intercambio de información entre nodos personales. La UCL, gracias a este adaptador, incluye la seguridad como una métrica más a la hora de seleccionar qué nodos forman parte del canal de comunicaciones. Esto se logra empleando la lista de nodos cuya identidad ha sido verificada como base para la generación de la ruta a un destino específico. Por supuesto, se podrán emplear otros nodos bajo la responsabilidad del usuario.

3.4.2.6.2. Optimización de rutas

Entre los AdP adicionales se pueden incluir todos aquellos que buscan la optimización de la ruta o el mecanismo de transmisión de los paquetes. La UCL ofrece la posibilidad de gestionar múltiples interfaces, lo que hace que pueda existir más de una opción para enviar datos entre un par dado de nodos.

Teniendo en cuenta el destino y la información recogida a través de los ARR (estado del canal, ancho de banda, etc.), se derivan muchas alternativas. Ponderando la información disponible con el perfil del usuario es posible seleccionar diferentes metodologías de transmisión, buscando la más óptima entre ellas. Algunas de las posibilidades, que con ayuda de la gestión inteligente de las interfaces de red se pueden implementar, son:

- Multiplexación de tráfico usando varios canales de transmisión simultáneamente.

- Selección del mejor enlace considerando múltiples métricas como SNR, ancho de banda, paquetes y/o tramas perdidas, etc.
- Selección del enlace más seguro basándose en la relación de confianza establecida entre los nodos.
- Priorización de flujos de tráfico asignados a una misma interfaz de red.

La validez de estas soluciones ha sido analizada y confirmada experimentalmente en [105, 106] y algunas de ellas se describirán con mayor detalle en el capítulo 6.

3.5. Capa de Abstracción a Nivel de Red

Hasta el momento todas las capas de abstracción definidas, cada una a su nivel, buscan proveer conectividad entre los nodos de un usuario de forma transparente y segura. El nivel de red de una PN no puede sino mantener dicho enfoque y debe ser tan independiente como sea posible de los niveles de enlace subyacentes de manera que tanto las tecnologías de comunicaciones actuales como las que surjan en un futuro puedan ser soportadas sin tener que realizar adaptaciones.

Si con la ayuda del nivel de conectividad y la UCL se logra establecer canales de comunicaciones seguros entre nodos personales, a nivel de red, dentro de la Capa de Abstracción a Nivel de Red (figura 3.12), el objetivo es hacer colaborar a grupos de nodos personales y aislar la comunicación entre esos nodos de la de otros usuarios. Parece claro que los nodos más cercanos se organizarán en *clusters* bien de forma automática o dirigida por el usuario. Dentro de los *clusters*, los nodos podrán comunicarse entre sí sin tener que apoyarse en nodos externos. De esta forma se logra proteger la comunicación y los mecanismos de organización, al circunscribirlos a los propios nodos personales dentro del entorno local.

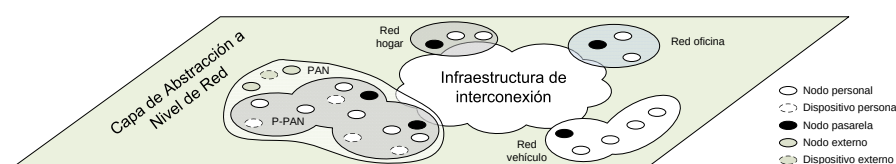


Figura 3.12: Capa de Abstracción a Nivel de Red

La PN se basa en el hecho de que el conjunto de dispositivos y nodos de usuario debe ser contemplado como una única entidad por éste; por ello, no tiene sentido como un conjunto de *clusters* inconexo sin posibilidad de comunicarse entre sí. Por esta razón, desde la Capa de Abstracción a Nivel de Red, se tiene que plantear un procedimiento para interconectar las diferentes agrupaciones de nodos de usuario.

Los conceptos de P-PAN, *cluster* y PN se definen y tienen sentido a nivel de red. Los *clusters*, incluyendo la P-PAN, operan como entidades autónomas en este nivel. Por tanto, la PN, entendida como la combinación de la P-PAN y el resto de los *clusters* de usuario, es una única red personal segura, considerando seguridad no sólo como privacidad (desde la perspectiva del usuario), sino también como robustez y resistencia a ataques desde el exterior. En ella, los *clusters* de usuario estarán conectados mediante canales seguros a

fin de garantizar el intercambio seguro de información entre ellos. La idea subyacente es generar una red virtual que, manteniendo el alto grado de seguridad de la PN, facilite que las comunicaciones entre cualquier nodo de la PN de un usuario sea independiente de su localización. Por lo tanto, la Capa de Abstracción a Nivel de Red debe además soportar un escenario de movilidad, tanto en término de *clusters* como de los nodos que los conforman, los cuales podrán pasar de uno a otro *cluster* de usuario de manera transparente.

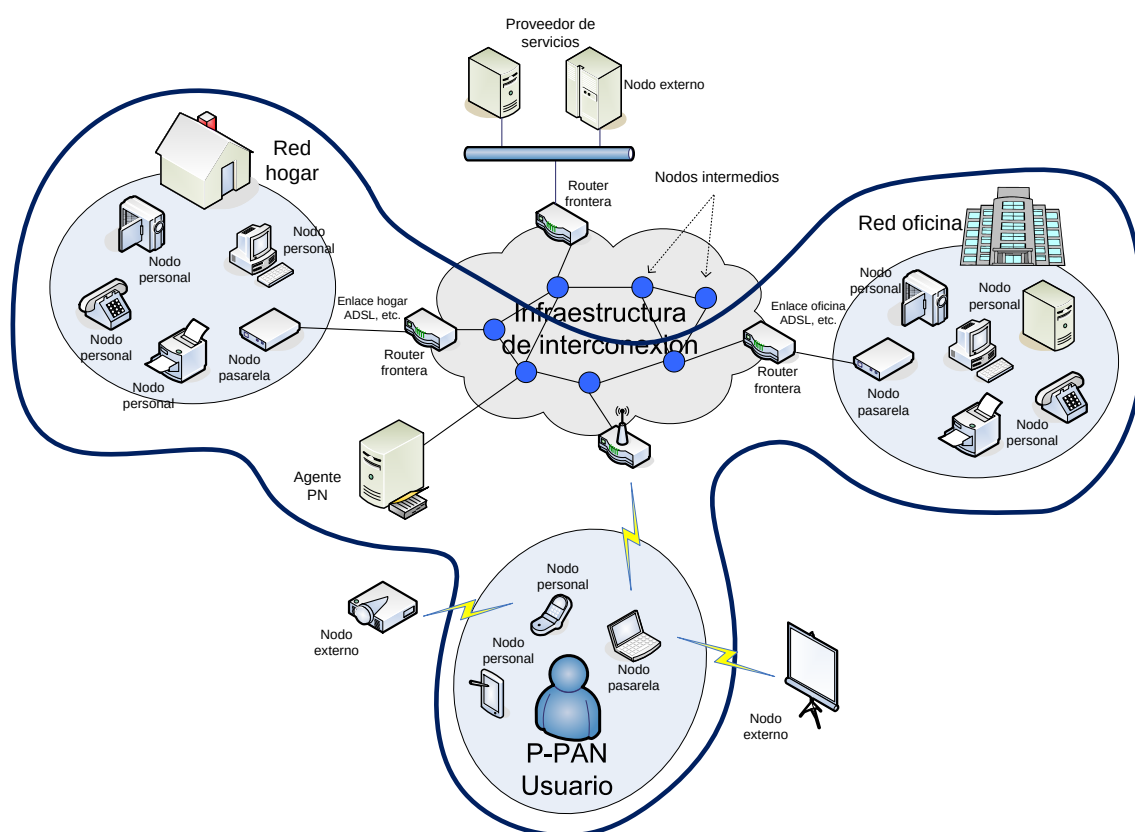


Figura 3.13: Arquitectura de nivel de red de una PN

En la figura 3.13 se muestra la arquitectura de alto nivel propuesta, representada tomando como base el escenario de la vida cotidiana de un usuario. Según esta representación, la red del hogar de una persona constituye un *cluster*, la red dentro del vehículo otro, la WPAN alrededor del usuario otro y así sucesivamente.

A diferencia de otras descripciones de *cluster* o PAN [74] que consideran el *cluster* en función del radio de cobertura como un conjunto pequeño de nodos dentro de un espacio geográficamente limitado (p. ej. 10m), el concepto de *cluster* dentro de la PN va mucho más allá. Un *cluster* en una PN se basa en la conectividad física y en el concepto de propiedad; es distribuido y sigue un enfoque multisalto proactivo basado en la relación de confianza entre sus miembros. Además, tiene en cuenta la heterogeneidad, se adapta a los cambios y no depende de la infraestructura para tener entidad propia. Si a esto se le une la garantía de privacidad dentro de él, se cumplen todos los requerimientos impuestos por el concepto de PN. Es por estas razones que el tamaño de los *clusters* dentro de una PN

no está restringido inicialmente en número de nodos ni en área de cobertura. Un *cluster* puede extenderse siempre que los nuevos nodos o dispositivos personales sean accesibles empleando una interfaz inalámbrica PAN.

Los *clusters* operan de forma autónoma como redes locales. Disponen de su propia metodología de encaminamiento, direccionamiento, procedimientos de auto-configuración, etc. Aunque todos los *clusters* y, en particular, la P-PAN (el *cluster* más cercano al usuario que se describirá en la siguiente sección) pueden desplazarse tanto geográficamente como lógicamente y, por tanto, modificar su punto de contacto o enlace con el exterior, la PN siempre debe mantenerse como una única entidad. Es por tanto esta capa sobre la que deben implementarse las soluciones de movilidad y seguridad que den soporte al mantenimiento de la PN.

En este sentido, la aproximación seguida para desplegar el concepto de PN es implementar la PN como una red superpuesta¹ segura y con capacidad para auto-configurarse y organizarse. Esta red superpuesta, que estará constituida por todos los nodos que pertenezcan a esa PN y en la cual se comunicarán libremente, compartiendo servicios y aplicaciones, tendrá su propio direccionamiento privado, logrando así confinar las comunicaciones entre nodos personales en ella.

Para establecer las comunicaciones entre los nodos dentro de la red superpuesta que conforman se necesita definir las metodologías de encaminamiento y direccionamiento a seguir. La PN está concebida de forma que debe ser capaz de encaminar paquetes de información por el camino más seguro y óptimo entre cualesquiera dos nodos dentro de ella. A partir de la arquitectura definida para la PN, parece que la opción más óptima sea definir un encaminamiento jerárquico, manteniendo un direccionamiento único asociado a cada PN y diferenciando la comunicación intra-*cluster* e inter-*cluster*.

En las siguientes secciones se muestran los mecanismos de interacción entre nodos dentro de la Capa de Abstracción a Nivel de Red. En este sentido, se describirán los procesos de formación y mantenimiento de la P-PAN, como desencadenante de la PN, y de la propia PN.

3.5.1. Formación de *clusters* y de la P-PAN

La formación de los *clusters* en una PN es puramente local y no requiere soporte por parte de la infraestructura. Los *clusters* son dinámicos por naturaleza; sus nodos se encienden y se apagan; otros se adhieren en itinerancia; se disocian cuando una persona selecciona un conjunto de nodos y los desplaza, dejando al resto operando entre sí o se fusionan, por ejemplo, cuando al llegar a casa la P-PAN se une al *cluster* del hogar.

La P-PAN es un *cluster* especial y único formado por el conjunto de nodos y dispositivos alrededor del usuario. Se trata del *cluster* más dinámico dentro de la PN no sólo en cuanto a movilidad sino también en cuanto al número de nodos y su capacidad de reconfiguración. El usuario se encuentra en constante movimiento portando sus equipos preferidos tales como

¹Una red superpuesta (*overlay network*) es una red virtual de nodos enlazados lógicamente, que está construida sobre una o más redes subyacentes. Su objetivo es implementar servicios de red que no están disponibles en la/s red/es subyacente/s. Las redes superpuestas pueden apilarse de forma que tengamos capas que proporcionen servicios a la capa superior.

el teléfono móvil, portátil, etc. No obstante no siempre lleva consigo el mismo conjunto de dispositivos, por lo que se puede considerar que la P-PAN está en continua reconfiguración, agregando nuevos nodos o disgregándose. Por estas razones, requiere un tratamiento específico.

Para añadir un nuevo dispositivo o nodo a la PN, éste debe haber sido inicializado como nodo personal por el usuario, procedimiento que requiere la interacción directa del usuario con su dispositivo. Por tanto, si ese nuevo nodo se conecta a la PN inmediatamente después de su inicialización, éste no sólo formará parte de la PN, sino que además pasará a ser parte de la P-PAN.

Introducir nuevos nodos en la PN supone definir la relación de confianza a largo plazo con cualquier otro dispositivo de la misma PN. Como resultado del procedimiento de marcado (*imprinting*) [107, 108] se genera una clave o secreto compartido entre cada par de nodos (*long-term pair-wise shared key*). La combinación de esa clave con un identificador único para cada nodo permite que dos nodos cualesquiera puedan descubrirse, identificarse y autenticarse entre ellos. Este proceso es la base para la creación de un enlace seguro entre los nodos y así habilitar la comunicación segura dentro del *cluster*. Los detalles de este proceso se describen en el capítulo 4.

La propia naturaleza de la P-PAN, como un *cluster* heterogéneo de generación espontánea, requiere la utilización de protocolos de encaminamiento multisalto de baja latencia y rápida respuesta, que no supongan una gran sobrecarga y permitan la inclusión, en los casos que se requiera, de información de QoS. Los protocolos de encaminamiento ad-hoc proactivos son los que mejor se adaptan a estos requerimientos. Por un lado encajan en los procedimientos de formación y mantenimiento del *cluster*, pues generan actualizaciones de rutas y del estado de la red ante la aparición de nuevos enlaces y/o destrucción de los existentes (los nodos se desplazan y se encienden y apagan). La rápida respuesta ante cambios y la baja latencia son aspectos inherentes a los protocolos proactivos. Además, el hecho de disponer de información actualizada en cada nodo permite la ejecución de algoritmos de decisión para seleccionar las rutas más óptimas. La P-PAN no define un protocolo específico a emplear dado que cualquiera dentro del ámbito de trabajo del grupo MANET puede ser válido cumpliendo las premisas anteriores.

Sin embargo, si a la heterogeneidad de interfaces de comunicaciones existente dentro del *cluster* se unen las especiales características en cuanto a qué nodos pueden formar parte del camino de comunicaciones entre dos nodos, hace que los mecanismos tradicionales de encaminamiento no se adapten totalmente a este entorno. Existen numerosas similitudes entre las PN y las redes MANET, tales como el comportamiento dinámico, la espontaneidad en su creación, etc. Pero, al no cumplir con algunos aspectos concretos de la PN, las soluciones MANET no pueden ser adoptadas directamente. Por ejemplo, en el caso de una P-PAN o cualquier *cluster*, se requiere tener conocimiento del número de nodos personales y del estado de los enlaces entre ellos. Las implementaciones estándar de los protocolos MANET no incorporan este tipo de descubrimiento ni emplean métricas propias de la PN para determinar las rutas.

Es en este punto donde entran en juego el papel de la UCL y el paradigma de optimización intercapas. La UCL incorpora los mecanismos tanto para proactivamente identificar los nodos personales en las proximidades, como para publicar esa información. Por tanto, de

forma genérica, bastaría una adaptación de las implementaciones de los protocolos proactivos para emplear la base de datos de nodos vecinos de la UCL como ayuda a la integración de las soluciones MANET en el ámbito de la PN.

Dentro del trabajo de esta tesis, así como en el marco del proyecto MAGNET, se ha integrado satisfactoriamente la UCL con protocolos de encaminamiento ad-hoc como *Wireless Routing* [109, 110] o *Ad hoc On Demand Distance Vector* (AODV) [111], demostrando esta operativa.

Los protocolos proactivos normalmente difunden mensajes que contienen información del nodo emisor y del vector de distancias. Especialmente en la P-PAN y demás *clusters* de la PN, estos paquetes deben ser transmitidos cifrados y firmados, de forma que se garantice no sólo la integridad de la información sino también la de la propia red. Idealmente, cada vez que una actualización de información de encaminamiento se envía, el nodo emisor solicita una confirmación de la recepción de dicho mensaje de actualización a los destinatarios, asegurando la correcta recepción y futura aplicación de los nuevos datos. Por esta razón, para el caso de la P-PAN y de forma genérica en toda la PN, se postula el empleo del protocolo *Wireless Routing*, al incorporar esos mecanismos de confirmación. El uso de este protocolo es meramente ejemplificativo, siendo posible, como ya se ha mencionado, emplear cualquier otro protocolo. El resultado del intercambio de la información de los mensajes de encaminamiento es que todos los nodos de los *clusters* tienen conocimiento actualizado del camino a emplear para alcanzar otro nodo.

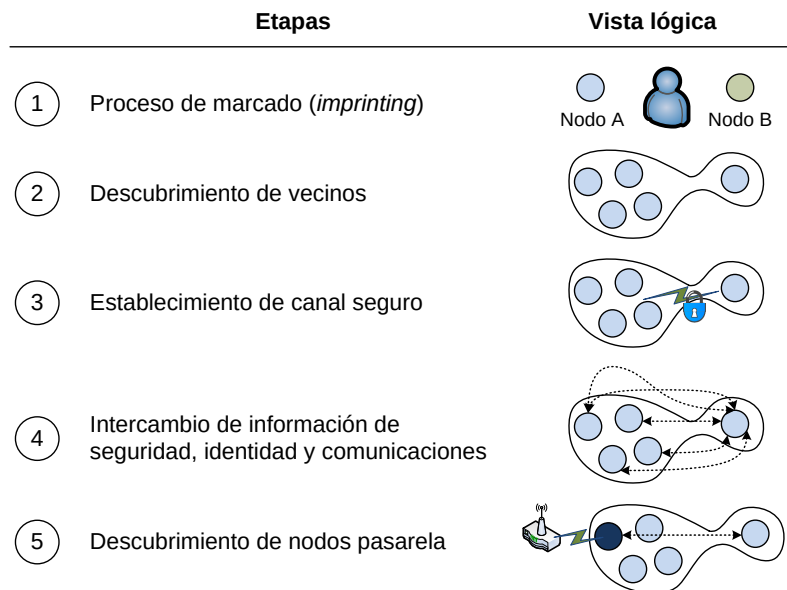


Figura 3.14: Proceso de formación de la P-PAN

Para hacer que los nodos de un *cluster* se comuniquen con los de otros *clusters*, cada *cluster* debe definir al menos una pasarela de entrada/salida o *gateway*. Estos nodos permiten la conexión del *cluster* con Internet y/o con el resto de la PN. La identidad de dichos nodos debe ser difundida a todos los nodos del *cluster*, siendo los mensajes de encaminamiento el medio ideal para incluir este tipo de información. Estos nodos deben soportar funcionalida-

des específicas como traducción de direcciones de red (NAT, *Network Address Translation*), creación, configuración y mantenimiento de la conexión entre *clusters*, filtrado de tráfico entrante, etc. Serán los *gateways* los que hagan frente a la movilidad inherente en la PN, actualizando donde corresponda la referencia del *cluster* al moverse entre redes y el listado de nodos personales bajo su control, para mantener la unidad de la PN.

Dada la carga adicional que dichos nodos tendrán que soportar, se recomienda que los nodos que se seleccionen como pasarela sean algunos de los nodos que dispongan de mayores capacidades (cómputo, comunicaciones, etc.). Sin embargo, la decisión final vendrá supeditada por las capacidades de comunicaciones que incorporen, ya que éste es el aspecto diferenciador con el resto de los nodos del *cluster*. La tarea de identificar los nodos más adecuados se realizará desde la capa de contexto. Haciendo uso de la interrelación existente entre las capas de red dentro de la PN y considerando también las preferencias de usuario, como el coste de la conexión de banda ancha, etc., se podrá determinar la idoneidad de un nodo pasarela.

En la figura 3.14 se muestra gráficamente un resumen del procedimiento de formación de la P-PAN y por extensión de cualquier *cluster*.

3.5.2. Formación de la PN

Una vez que los nodos se han organizado en *clusters*, para que la PN se pueda dar como constituida deben establecerse enlaces entre ellos. Tras la etapa de creación y organización, sólo resta el mantenimiento transparente de la estructura generada y garantizar la seguridad de uso para el usuario. A continuación se describirán los componentes que aseguran la realización de estas tareas.

Al desplazarse los nodos, los *clusters* de los que forman parte se mueven con ellos. El grado de movilidad del *cluster* como un todo dentro de la PN no es comparable a la movilidad que se da dentro de cada *cluster*. Mientras que se puede considerar el dominio de la PN como algo estático, los *clusters* internamente son muy dinámicos. Aceptando la anterior afirmación como válida, no es necesario que el protocolo de encaminamiento que permita la interconexión entre los *clusters* reaccione de forma tan rápida ante los cambios. Es más, toda vez que los *clusters* están formados y conectados cobra mayor importancia el hecho de que las transferencias entre ellos no conlleven una elevada latencia ni sobrecarga de red. En este sentido parece adecuado que exista una entidad, conocida por todas las pasarelas, que haga las veces de repositorio de puntos de enlace, incluyendo sus identificadores, sus direcciones de acceso, etc. y que facilite entre otras cosas el establecimiento y búsqueda de nuevos enlaces. Este repositorio constituye una nueva entidad dentro de la PN denominada agente de la PN.

El agente de la PN mantiene información actualizada de los puntos de acceso a los *clusters*, acelerando los procesos de descubrimiento y formación de los enlaces entre ellos. Esta funcionalidad se puede asemejar a la del agente local (HA, *Home Agent*) en las soluciones basadas en MIP [15, 16]. La forma en la que esta entidad lógica se implemente no es relevante, siempre y cuando exista al menos un agente por PN y proporcione la funcionalidad deseada. El agente de la PN podría ser desplegado como un elemento fijo dentro de alguno de los *clusters* estables de la PN de un usuario. Pero, considerando el dinamismo de la PN,

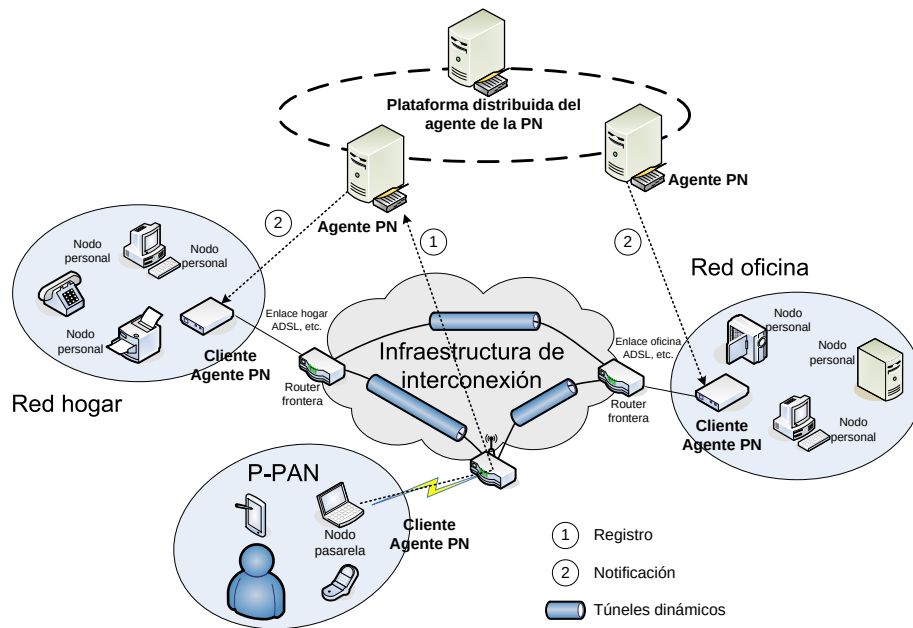


Figura 3.15: Plataforma distribuida del agente de la PN

se recomienda que su funcionalidad sea distribuida en la red con el objeto de reducir la influencia de errores de acceso o disponibilidad, tal como se refleja en la figura 3.15. En este sentido es importante reseñar que la misma infraestructura se podría emplear para dar soportes a múltiples PN, por ejemplo delegando la gestión de los agentes de las PN en un tercero, p. ej. un proveedor de confianza.

La conectividad entre los *clusters* sólo se puede establecer si son capaces de localizarse entre ellos. Por tanto, tan pronto se habilite la comunicación con la infraestructura deben registrarse en el agente de la PN. Cada nodo pasarela deberá ejecutar el cliente del agente de la PN, quien guiará las tareas de registro. Adicionalmente este cliente participa en el mantenimiento de la PN gestionando las notificaciones que se envíen desde la parte servidora informando del estado del resto de los *clusters*. La identidad del agente de la PN debe ser conocida por cada nodo pasarela, siendo tras el marcado del nodo el momento más adecuado para grabar esta información. La disponibilidad de un *cluster* vendrá definida por el envío periódico de mensajes de mantenimiento de enlace vivo (*keep-alive*) incluyendo la información de los puntos de conexión del *cluster*.

Tanto en el momento del registro como en las sucesivas actualizaciones de estado, los nodos pasarela dan a conocer el estado del *cluster* al que representan. Los mensajes deben incluir la identidad del *cluster*, la dirección de los nodos pasarela habilitados y la composición de la agrupación, es decir, el conjunto de identificadores de los nodos personales que la conforman. Opcionalmente pueden incluir información estadística (p. ej. de uso), localización, estado de los nodos, servicios disponibles, etc. Estos datos serán empleados por las Capas de Abstracción de Nivel de Servicio y de Contexto para adecuar la operativa de la PN en cada momento. En este sentido, una funcionalidad adicional que el agente de la PN puede incorporar, en combinación con el contexto de la PN, es la toma de decisiones de

balanceo de carga si observa que hay sobrecarga en alguno de los túneles o bien habilitar el contacto entre los nodos gestores de servicios (SMN, *Service Management Node*) o los nodos gestores de contexto (CMN, *Context Management Node*).

La información recibida por el agente de la PN se remite al resto de los *clusters* registrados, de forma que ejecuten las acciones oportunas de gestión de los túneles seguros, establecimiento y/o mantenimiento. El empleo de túneles cifrados permite encapsular el tráfico intra-PN, protegiéndolo de posibles escuchas o ataques externos. Si bien nadie puede garantizar que la infraestructura empleada para conectar los nodos sea completamente segura, si se puede afirmar que los mecanismos de comunicación de la PN en sus diferentes niveles al menos garantizan la integridad y confidencialidad extremo a extremo.

La creación de estos túneles implica el intercambio entre los nodos extremos de la información necesaria para establecer ese canal seguro, es decir, el tipo de entidad, modo de encapsulación que se desea aplicar y las necesidades de conectividad adicionales (soporte NAT, etc.). Toda esta información permitirá la generación de claves temporales con las que cifrar y validar el tráfico que circule por el túnel. De forma genérica se recomienda el uso de *IP Secure* (IPSec) o bien de soluciones basadas en *Secure Sockets Layer* (SSL). Usualmente, estos procedimientos estándar operan sobre TCP. Sin embargo, dado que los *clusters* pueden obtener conectividad a través de redes privadas con salida a Internet habilitada mediante NAT, se establece la posibilidad de desplegar túneles sobre *User Datagram Protocol* (UDP).

Con los túneles formados, se habilita el intercambio de datos entre los nodos de los *clusters*. El reporte periódico remitido por los nodos pasarela, en el que se incluye un listado de los nodos pertenecientes a su *cluster*, se emplea para actualizar las tablas de rutas de los nodos pasarela remotos. Esto hace que en el caso de tener que transmitir información hacia nodos de otros *clusters*, la ruta se pueda establecer inmediatamente. La PN puede optar también por soluciones reactivas redundando en una mayor latencia del envío, al tener que realizar una búsqueda de la localización del nodo. La información que se almacene en la caché tendrá una vida limitada.

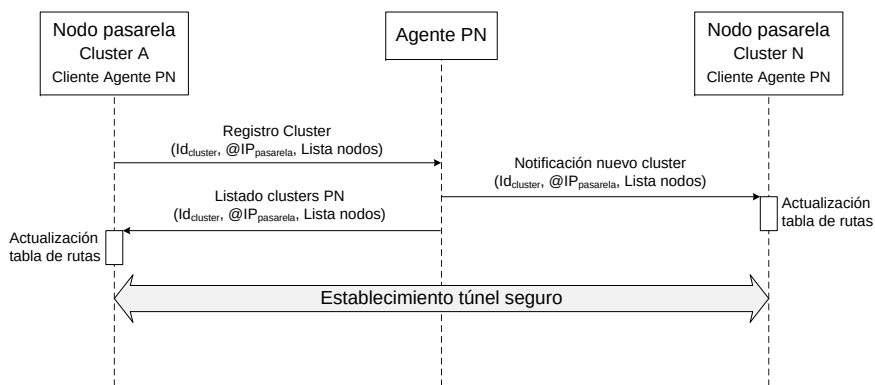


Figura 3.16: Evolución del procedimiento de conexión entre *clusters*

En la figura 3.14 se representa el flujo de información intercambiado entre los diferentes nodos de la PN durante la formación de las conexiones entre *clusters*.

Con el objetivo de tratar de liberar a los nodos pasarela de la complejidad y sobrecarga que implica la gestión de los túneles, se plantea, al igual que ocurre con el agente de la PN, la opción de ceder parte de las funcionalidades a una TTP. En este sentido, se podría extender la misma relación de confianza que establecen los nodos de un usuario a proveedores de red que realicen todo el despliegue y gestión de las comunicaciones intra-PN de forma segura.

El concepto de *router* frontera o *router* de acceso a la PN (*edge router*) [112] se define para dar cabida a esta nueva funcionalidad. Se encargan de gestionar el encaminamiento y redirección de paquetes de forma que uno o varios *clusters* tengan acceso a la infraestructura de red o red troncal, salvaguardando la privacidad de las comunicaciones. Los túneles o enlaces virtuales en esta nueva configuración se establecerán entre los *routers* de acceso, liberando de esta forma a los nodos pasarela de estas funcionalidades, reduciéndolas prácticamente a la redirección de tráfico, operativa ésta implementada por defecto en casi cualquier nodo. Serán estos *routers* los que informarán al agente de la PN de las modificaciones en la configuración de los *clusters*.

En caso de optar por una opción distribuida, sin agente de la PN, los nodos pasarela de cada *cluster* se organizarán generando una red P2P e intercambiarán sobre ella la información de contacto. Esta solución, si bien evita la necesidad de una entidad central de gestión, supone incrementar las funcionalidades necesarias en los nodos pasarela y complicar la gestión de la PN con un aumento considerable del tráfico de gestión entre los nodos personales.

En ocasiones los *clusters* pueden no tener acceso a la infraestructura, bien porque ningún nodo disponga de una interfaz de acceso de banda ancha o porque la conexión en un momento puntual no esté activa. Para solventar estas situaciones, está prevista la interacción con otros *clusters* dentro de su entorno cercano, extendiendo el uso de los mecanismos de comunicación ad-hoc intra-*cluster* o incluso llegando a fusionarse. Adicionalmente puede optarse por el empleo de nodos externos que hagan las veces de intermediario. Esta última opción no garantiza la seguridad completa del enlace de comunicaciones, pero al menos lo habilita y no compromete la seguridad extremo a extremo.

3.5.3. Direccionamiento en una PN

Los nodos que componen la PN forman parte de una red virtual. No obstante no existe impedimento para que esos nodos se comuniquen fuera de la PN, siempre teniendo en cuenta que esas comunicaciones no mantendrán los altos niveles de seguridad de la PN. Por tanto, cada nodo personal tendrá al menos dos direcciones, una global de la red enrutable desde Internet o perteneciente a la red privada a la que esté conectado y otra específica de la PN. Para evitar la confusión, a partir de este punto se referirá a la dirección específica de la PN como dirección PN o personal.

Dentro del ámbito de la PN se pueden plantear diversos esquemas de direccionamiento: plano, jerárquico, etc. Cualquiera de las opciones que se seleccione tiene sus ventajas e inconvenientes. De una parte, el direccionamiento plano no proporciona información relativa al emplazamiento del nodo personal, pero en cambio facilita la identificación de éste dentro de la PN y habilita un soporte en movilidad más sencillo [113], pues asigna la misma dirección independientemente del *cluster* en el que se encuentre el nodo. Adicionalmente aquellos

servicios que no tengan soporte para manejar el cambio de dirección durante una sesión se verán beneficiados por este modo de direccionamiento. Por el contrario, la escalabilidad y complejidad de las tablas de rutas se ve afectada de forma negativa.

El direccionamiento jerárquico basado en *clusters* ofrece, en cambio, una gestión de las rutas más ordenada al incluir en la dirección de los nodos el prefijo del *cluster* en el que están. La reducción en cuanto al número de entradas en la tabla de rutas pasaría de $O(\text{número de nodos personales})$ a $O(\text{número de nodos pasarela})$, pero, por otra parte, la fusión o disociación de un *cluster* sería comparativamente más costosa.

En cualquiera de los casos, todo nodo de una PN tiene una única dirección personal habilitada. Para la asignación de dicha dirección se pueden considerar dos opciones, dinámica o estática. En el caso dinámico es necesario incorporar algún mecanismo que permita la detección de direcciones duplicadas (DAD, *Duplicate Address Detection*), de forma que se garantice que dos nodos de la PN no comparten la misma dirección. Estos mecanismos se basan en la estabilidad de la definición de subred, algo que en entornos ad-hoc no se puede garantizar. En el caso de la PN no existe una limitación clara de la subred, teniendo que extender la comprobación al ámbito de toda la PN. La información residente en los nodos pasarela puede ayudar ya que contiene un listado de los nodos residentes en los *clusters*. No obstante, además de requerir acciones específicas del protocolo de encaminamiento, la información residente no tiene por qué estar complementada actualizada.

En esta situación se acepta como más efectiva la asignación de una dirección personal fija de forma estática y que ésta se mantenga invariante durante la vida del nodo personal. Sin embargo, dependiendo del esquema seleccionado, ciertas secciones de esta dirección podrán modificarse para adaptarse a la movilidad del nodo dentro de la PN.

En las implementaciones de la PN realizadas en el marco de este trabajo se opta por el direccionamiento plano dentro de toda la PN como opción más adecuada, de forma que los dispositivos y nodos de usuario mantengan su dirección invariante cuando se desplacen dentro de la PN, si bien el formato de direccionamiento que se describe a continuación está llamado a soportar ambas soluciones.

3.5.3.1. Formato

La PN de un usuario puede incluir un gran número de nodos. El direccionamiento basado en IPv4 permite adjudicar un conjunto limitado de direcciones y el soporte ofrecido para asignar varias direcciones a un mismo interfaz o nodo no es idóneo. Por el contrario, IPv6 no presenta apenas limitaciones en estos aspectos y su diseño facilita además la definición de esquemas de direccionamiento jerárquico.

Por estas razones el esquema de direccionamiento empleado dentro de la PN se basará en IPv6, si bien se deja abierta la puerta a proporcionar soluciones sobre IPv4 en despliegues a pequeña escala o allí donde no existe soporte IPv6. En la figura 3.17a se muestra el formato de una dirección PN donde:

- Prefijo de PN: puede estar enmarcado dentro del espacio de direccionamiento *Unique Local IPv6 Unicast* [114] o bien dentro del global. Su valor se obtiene a partir del identificador de la PN.

- Identificador de subred: puede emplearse para referirse al *cluster* en el que está el nodo. Se reserva el valor “todo a ceros” para el caso de emplear un esquema de direccionamiento plano.
- Identificador de la interfaz: generado a partir de los 48 bits de dirección MAC de la interfaz[115]. La UCL habilita por defecto una única dirección MAC, aunque en caso de operar con varias se recomienda seleccionar alguna de las interfaces incluidas de fábrica en el *hardware* del nodo.

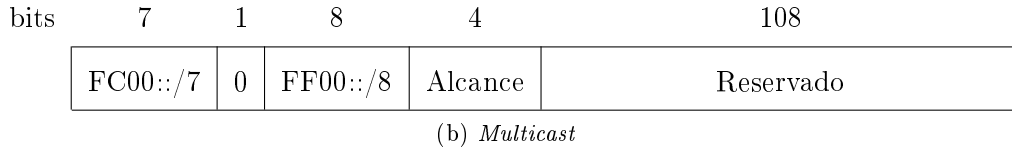
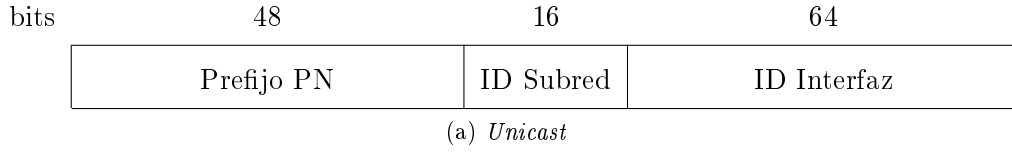


Figura 3.17: Formato de dirección personal

El conjunto de direcciones a emplear dentro de la PN no se puede reducir a direcciones *unicast*, sino que se debe reservar un subgrupo para realizar comunicaciones de difusión (*multicast* y *broadcast*) dentro de los *clusters* y para toda la PN. El formato definido para este conjunto de direcciones se describe en la figura 3.17b, donde el campo alcance indica el número de saltos o la distancia a la que el paquete se propaga y puede tomar los siguientes valores:

- 0x00 un salto
- 0x01 dentro del *cluster*
- 0x02 dentro de la PN
- 0x03-0x0F RFU

Los valores asignados al resto de los bits de la dirección fijan su condición de dirección de difusión, donde los 7 primeros denotan el uso de una dirección tipo *Unique Local IPv6 Unicast* y los 8 siguientes se fijan para diferenciarla de cualquier otra posible dirección personal. En este sentido, los bits menos significativos (bits 20-127), si bien por defecto son ceros, podrían incluir el prefijo de la PN, de forma que en el caso de habilitar comunicaciones entre PN o con los proveedores de servicio, se identifique el generador del tráfico de difusión.

Se debe prestar especial atención al algoritmo de transmisión de los paquetes de difusión en un entorno multisalto como es la PN. Una mala selección de la metodología puede provocar la inundación de la red con paquetes redundantes, reduciendo el rendimiento global. En este sentido, existen diversas soluciones [34, 116], si bien dentro de la PN la UCL

puede proporcionar un apoyo adicional incluyendo cabeceras extras en el paquete de datos que permitan un mayor control.

3.5.3.2. Asignación

La dirección personal se ha definido como la concatenación de un prefijo asociado a la PN y un identificador único asociado al nodo. Considerando que el espacio reservado para el identificador de la interfaz (64 bits) es suficientemente amplio, se puede garantizar la unicidad y globalidad de la dirección sin necesidad de tener que ejecutar procedimientos DAD.

Por tanto la asignación de una dirección a un nodo personal se reduce a la elección adecuada del prefijo de la PN. Desde la configuración por parte del usuario en el momento de introducir el nodo en la PN (p. ej. durante el procedimiento de *imprinting* [107]), pasando por la asignación por parte del agente de la PN, hasta una generación dinámica bajo acuerdo de todos los nodos, todas ellas son alternativas válidas para definir el prefijo. Aunque la última opción ha sido ampliamente estudiada [117] y se conocen diversas soluciones, su aplicación dentro de la PN puede resultar complicada ya que los nodos personales no conocen a priori qué grupos de nodos son los que forman parte del proceso de decisión. La variante del problema, conocida como búsqueda del consenso con participantes desconocidos (CUP, *Consensus with Unknown Participants*) [118], permite lograr el consenso en *clusters* con conexiones muy malladas, pudiendo ser adecuada en un entorno como el de la PN donde los nodos se mantienen fuertemente relacionados gracias al procedimiento de descubrimiento de vecinos.

No obstante, se ha considerado que el proceso de personalización de un nodo se erige como el momento más adecuado para definir el prefijo de la PN. Asistido por el usuario, el nuevo nodo establece la relación de confianza a largo plazo con un nodo personal. Este proceso puede extenderse intercambiando información estática, como es el prefijo de la PN.

Siguiendo esta estrategia, durante el primer proceso de personalización, que origina la PN, se genera el prefijo de ésta, que heredarán el resto de los nodos. El prefijo puede ser generado de forma local en el nodo, aleatorio o basado en información de usuario, o bien obtenido del agente de la PN. Buscando la unicidad y univocidad del prefijo entre diferentes PN, los agentes de las PN tendrán que confirmar la validez del prefijo. Son ellos los que conocen a los usuarios y, por tanto, los que pueden intercambiar información que permita comprobar que un determinado prefijo no haya sido asignado anteriormente.

Sin embargo, existe una situación particular a tener en cuenta. En el caso que dos nodos cualesquiera se personalicen de manera aislada (PN espontáneas), existe el riesgo de que al tratar de parearse con otros nodos de la PN tengan prefijos diferentes y por tanto formen dos PN diferentes. En estos casos, habiendo sido el usuario quien ha guiado los procesos de personalización, deberá ser él quien resuelva el conflicto sobrescribiendo el prefijo incorrecto y fundiendo las dos PN. La acción de unir las PN implica el borrado de los nodos de una PN y su personalización nuevamente dentro de la otra PN, es decir, establecer las relaciones de confianza a largo plazo. Esta tarea, si bien parece sencilla, es especialmente compleja a medida que el número de nodos en ambas PN aumenta.

Para evitar estos problemas se recomienda que tan pronto un nodo tenga conexión a

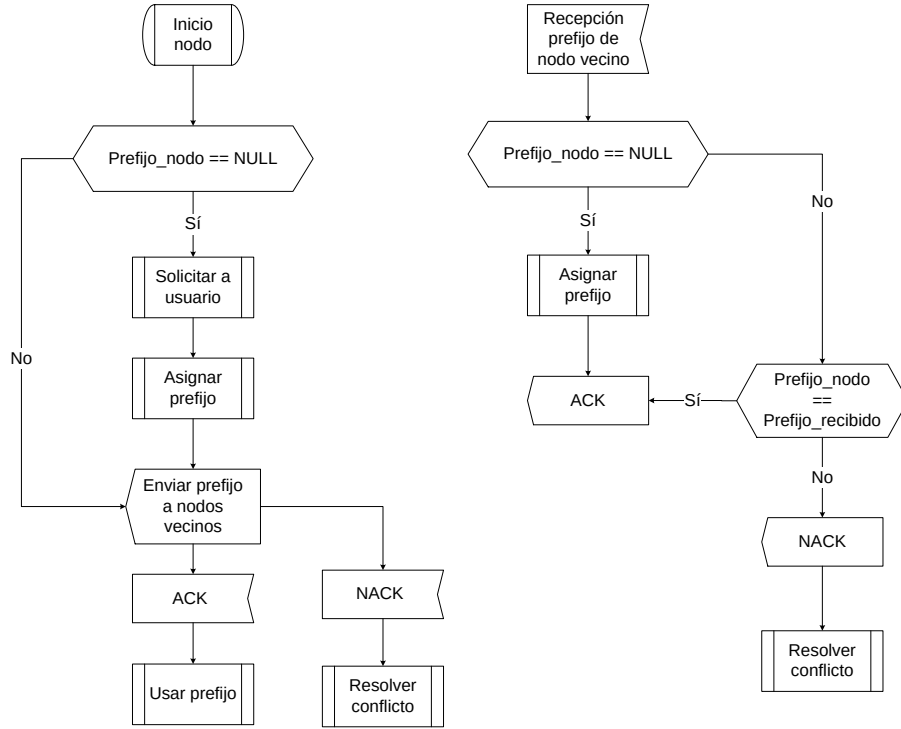


Figura 3.18: Diagrama de flujo de auto-configuración del prefijo de la PN

la infraestructura o bien pase a formar parte de un *cluster* con conectividad, actualice su estado en el agente de la PN. Como se ha venido describiendo, el delegar o apoyarse en el agente de la PN simplifica las tareas de gestión dentro de la PN. Así, si se diera un conflicto en el valor del prefijo entre dos nodos, será el agente de la PN quien dilucide el prefijo válido, por ejemplo en función del momento de registro.

En caso de emplear un esquema de direccionamiento jerárquico, el proceso de asignación del prefijo de la PN se mantiene invariante. Sin embargo, hay que considerar el procedimiento para asignar el prefijo del *cluster*. La definición del identificador de subred o *cluster* se realiza de forma dinámica, ya que los *clusters* se pueden generar y destruir continuamente, lo que hace inviable tener al usuario pendiente en todo momento. Será el nodo coordinador del *cluster*, es decir, aquel nodo con más capacidades, p. ej. un nodo pasarela, quien seleccione dicho prefijo. Ese prefijo se distribuirá dentro del *cluster* y se actualizará en el agente de la PN. No obstante, el encaminamiento en el ámbito del *cluster*, al usar un direccionamiento plano, no tendrá en cuenta este prefijo, cobrando únicamente sentido en el caso de comunicaciones inter-*cluster*.

3.5.4. Mantenimiento de la PN

Dentro de la PN, las transferencias inter-*cluster* se tratan de una forma similar a las intra-*cluster*. El nodo pasarela determina, en función de la dirección de destino, el *cluster* hacia el que redirigir el paquete. Desde el punto de vista de encaminamiento, los nodos pasarela se encuentran a un único salto de distancia entre ellos. Es más, cualquier nodo

remoto se encuentra virtualmente dentro del *cluster* local al ser el paquete con el direccionamiento personal encapsulado en el túnel y mantener el *cluster* remoto el mismo protocolo de encaminamiento intra-*cluster*. Este modo de operación hace que sea más sencillo gestionar la movilidad, ya que únicamente los nodos pasarela de cada *cluster* se verán afectados ante un cambio en las condiciones de acceso a Internet.

Una vez establecidos los túneles entre los *clusters*, para mantener la unidad de la PN se ha de mantener vivo el enlace. Los nodos pasarela y el agente de la PN monitorizan el estado de los túneles y actualizan las tablas de rutas, de forma que toda modificación de la situación de los nodos pasarela (canal de acceso externo) supondrá una renegociación del túnel.

En la figura 3.19 se representa el procedimiento de encaminamiento y gestión de túneles.

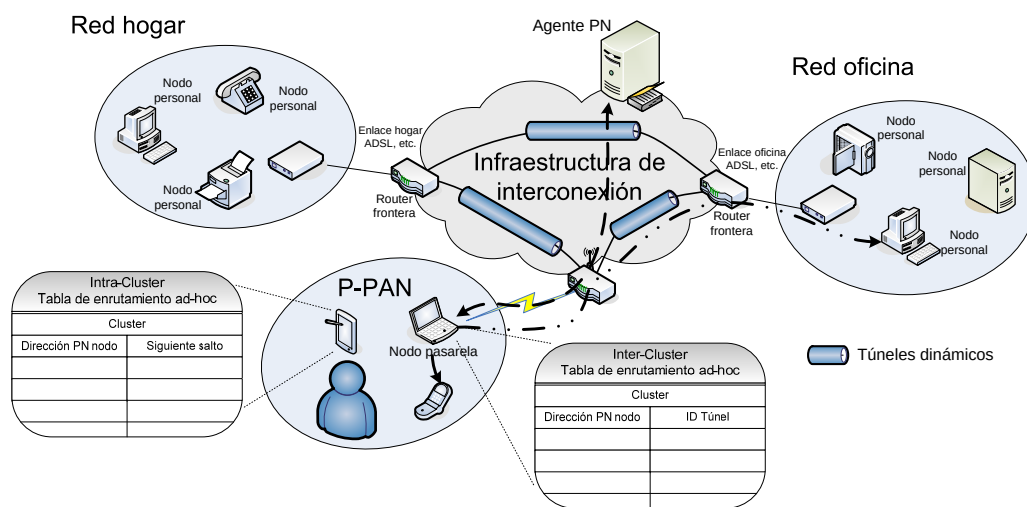


Figura 3.19: Gestión dinámica de los túneles y encaminamiento a nivel PN

La PN se origina como una red capaz de proporcionar una provisión de servicios segura y con una alta QoE. El mantenimiento de la sesión debe garantizarse incluso en movilidad. El esquema de direccionamiento privado seleccionado para la PN mantiene los identificadores de los extremos de la comunicación invariantes independientemente de la localización de los nodos. No obstante, el usuario puede experimentar una interrupción del servicio, cuya duración dependerá de la capacidad para recuperar la conectividad con la red y restablecer los enlaces virtuales. Los nodos pasarela o, en caso de que se estén empleando, los *routers* fronterizos pueden almacenar temporalmente paquetes y reenviarlos toda vez se haya restaurado el enlace. Este comportamiento puede ser de especial utilidad cuando se accede a servicios multimedia.

Para tratar de anticiparse a estas situaciones, es de gran utilidad la información adquirida por la UCL. El análisis del estado del canal radio empleado, a través del módulo GRR, permite detectar la degradación del mismo y adelantar alternativas de conexión e incluso asistir en el traspaso, como en la implementación estándar de Fast Mobile IP [119]. La Capa de Abstracción a Nivel de Contexto, que se describe más adelante, permite incorporar más información al procedimiento de toma de decisiones, adecuando el comportamiento a los requerimientos del usuario. En el ámbito de esta tesis se ha analizado el comportamiento

de la UCL para seleccionar óptimamente el canal radio a emplear (traspaso horizontal) basándose en la calidad del mismo (errores, seguridad, ancho de banda, etc.) [120] y cuyo detalle puede observarse en el capítulo 6. El planteamiento básico de una PN, tal como se ha descrito, supone el despliegue de un conjunto de entidades y funcionalidades que se asemejan a las proyectadas en MIPv6 [16]. Es por esto que se ha experimentado con el traspaso vertical entre tecnologías radio asistido por el usuario empleando MIPv6.

Señalar que el escenario en el que alguno de los *clusters* queda desconectado del resto de la PN no implica la división de la PN. Esta situación puede darse con la P-PAN, al ser el *cluster* con un mayor grado de movilidad. Aunque la P-PAN se separe del resto de la PN, la PN como tal seguirá manteniendo su identidad y los *clusters* seguirán siendo personales, con la peculiaridad de que en ese momento no estarán accesibles. Al ser el usuario quien guía el procedimiento de personalización, todos los nuevos nodos que personalice en esta situación adquirirán las características de cualquier otro nodo personal, con lo que al restaurarse la conexión con el resto de los *cluster*, podrán comunicarse con ellos de forma segura.

3.5.5. Comunicaciones con nodos externos

Hasta el momento se ha descrito la comunicación entre nodos personales. Sin embargo, una PN no está aislada y los nodos de un usuario pueden tener la necesidad de interactuar con otros fuera de su PN. A nivel de conectividad, siempre que compartan una tecnología de comunicaciones radio podrán establecer un enlace de comunicaciones en el que la seguridad no estaría garantizada. La Capa de Abstracción a Nivel de Red tiene, por tanto, que proporcionar los medios para hacer realidad esa comunicación.

La idea inicial pasa por extender la operativa por la cual una PN es capaz de comunicarse con la infraestructura. Pero en este caso las necesidades van más allá de la mera redirección de tráfico, ya que implica el uso y provisión de servicios a esos nodos.

Antes de proceder, hay que conocer las posibles localizaciones de estos nodos con respecto a la PN para diseñar una solución lo más global posible. Los nodos según su ubicación se pueden agrupar en tres grupos: aquellos que se encuentran en las inmediaciones de la P-PAN, los remotos próximos a un *cluster* y los conectados a la infraestructura.

La comunicación con los nodos externos en las proximidades de un *cluster* puede establecerse de forma directa. De forma guiada por el usuario o a través de mecanismos inteligentes se descubren los nodos y éstos pueden comunicarse. En este sentido, los nodos personales no emplearán ninguno de los mecanismos de seguridad establecidos para la operativa dentro de la PN, llegando incluso a emplear direccionamiento público de la red que compartan con el nodo externo. Un ejemplo de este tipo de situación es el caso en el que un turista quiera acceder a información de valor añadido de la ciudad (mapas, guía de eventos, etc.). En este escenario, en las proximidades de los postes informativos el usuario acercando su dispositivo descubre las direcciones de acceso a la información (p. ej. empleando tecnologías de campo cercano o códigos *Quick Response* (QR)) y descarga aquellos contenidos que desee.

En el caso que el nodo externo se encuentre conectado a la infraestructura, el mecanismo de interacción no es tan directo. El nodo personal tendrá que hacer uso de los nodos pasarela para establecer esa comunicación. Como alternativa, dado que la dirección del

nodo pasarela revela información sobre la localización del nodo personal, con el objeto de ocultarla, la comunicación se puede plantear a través del agente de la PN.

En todos los casos es recomendable que se empleen mecanismos que puedan comprobar la autenticidad del nodo externo. Para ello existe la posibilidad de extender el procedimiento de marcado o bien emplear autenticación y procedimientos de seguridad a nivel de servicio [107].

Aun así, el hecho de que un nodo externo sea el que inicie la comunicación hacia la PN presenta mayores problemas. El caso genérico implica el uso de un servicio provisto por un nodo personal, que el nodo externo haya descubierto a través de los mecanismos que se habiliten en la Capa de Abstracción de Nivel de Servicio. La PN es una red cerrada donde los puntos de interconexión con el exterior están muy limitados y para habilitar una comunicación el propósito de ésta tiene que estar bien claro. Toda vez se haya garantizado la seguridad de acceso, bien a través de los nodos pasarela, *routers* fronterizos o del agente de la PN, se permitirá el acceso al servicio seleccionado. Con el objetivo de mantener la privacidad, estos nodos ocultarán la identidad del nodo personal que provisiona el servicio. El empleo de estos nodos como pasarela de servicio supone la ruptura de la sesión extremo a extremo y puede no ser admisible en ciertas situaciones. Además de inhabilitar la seguridad que el servicio pudiera incorporar, existirá una degradación notable de la QoS para aplicaciones multimedia en tiempo real a causa del retardo introducido en las operaciones de redirección.

3.5.6. Flujo interno entre componentes funcionales de los nodos

Las descripciones realizadas se han realizado desde un enfoque de operativa de alto nivel sin profundizar en las relaciones entre los elementos funcionales o componentes que residen en cada nodo personal. Centrando la atención en aquellos nodos personales con capacidades IP, en la figura 3.20 se muestran las interfaces y las interacciones entre los diferentes módulos, proporcionando una visión más realista de qué componentes están a cargo de cada tarea y el flujo de mensajes entre ellos que hace posible el establecimiento y mantenimiento de la PN.

Durante el proceso de personalización del nodo, se fijan las claves bilaterales compartidas a largo plazo y el prefijo de la PN. El módulo de direccionamiento emplea dicho prefijo para definir la dirección personal del nodo y las direcciones de difusión de la PN. A partir de este momento el nodo personal puede comunicarse con el resto de los nodos de la red. Para ello primeramente tiene que descubrirlos, tarea que se lleva a cabo gracias al módulo de descubrimiento de vecinos de la UCL. Por cada nodo vecino se establecen unas claves de sesión temporales que habilitan un canal seguro de comunicaciones entre los nodos. Tanto ante el descubrimiento de un nuevo nodo como ante la rotura de un enlace, el módulo de descubrimiento de vecinos actualiza la tabla de encaminamiento interna. Todo paquete que se remita a nodos dentro del *cluster* se transmite a través de la UCL, quien cifra los datos y selecciona la interfaz óptima para el envío, modificando los datos del paquete (cabecera MAC, etc.) según corresponda.

En los nodos pasarela la operativa anterior se mantiene, pero se incorporan módulos adicionales que permiten el control de las interfaces de banda ancha y la gestión de los túneles

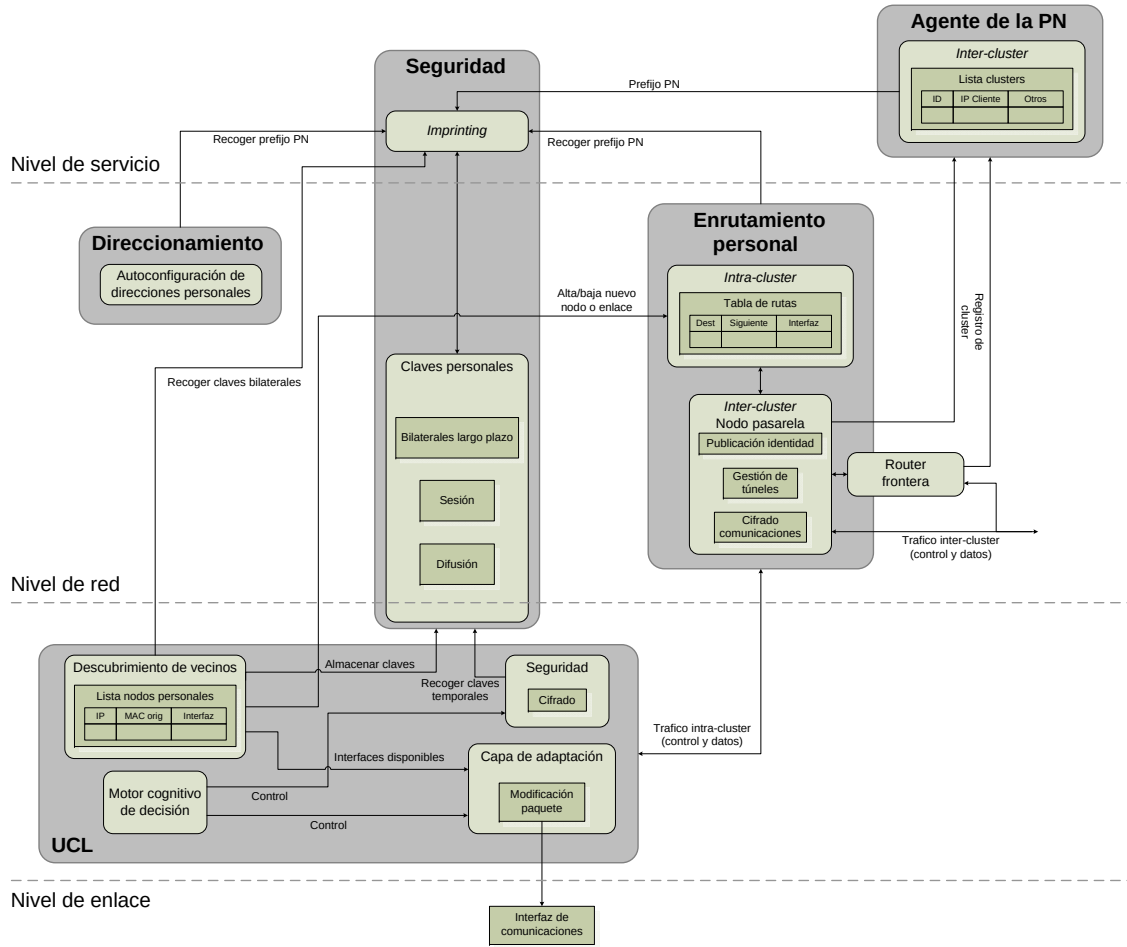


Figura 3.20: Interfaces de interacción en un nodo personal

o la comunicación con los *routers* fronterizos. El módulo de encaminamiento determina, a partir de la dirección destino, el *cluster* al que tiene que ser remitido el paquete. Encapsula dicho paquete en el túnel apropiado y lo envía. Adicionalmente el nodo pasarela periódicamente remite información de presencia, de forma que los nodos personales de su *cluster* y los nodos pasarela de los otros *clusters* actualicen su tabla de rutas.

3.6. Capa de Abstracción a Nivel de Servicio

Una PN define un ambiente inteligente que rodea al usuario y le ofrece la posibilidad de acceder a sus recursos de forma segura y transparente. Entre los recursos de usuario, además de los recursos físicos que proporcionan la conectividad, alojamiento, etc., se encuentran los servicios ofrecidos. Si bien dentro de una PN los servicios ofertados se limitan a aquellos considerados de usuario, éstos deben presentarse y operar adecuándolos a los requerimientos y necesidades específicas definidas por las condiciones de contorno del usuario.

Dentro de su PN el usuario actúa como mero consumidor de los servicios desplegados en sus nodos. Muchos de estos servicios pueden haber sido definidos por el propio usuario

componiendo diferentes funcionalidades existentes para dotar de un valor añadido. Adicionalmente, la estructura de una PN permite el acceso a aplicaciones de terceros. En este caso, el rol que desempeña se puede considerar como de consumidor. No obstante, ya se ha comentado que puede darse la posibilidad de que nodos externos estén interesados en el uso de servicios desplegados dentro de la PN, actuando entonces el usuario como proveedor. En consecuencia, el entorno integral de la PN debe ampliarse más allá del tradicional consumo de servicios en movilidad a su creación, gestión y provisión; se trata de una concepción del usuario que se denomina *prosumer*, es decir, el papel del usuario presenta una doble vertiente, tanto como generador y proveedor de servicios como consumidor de ellos. Aunque en el capítulo 5 se detallarán en mayor profundidad las implicaciones de esta nueva concepción del usuario, a continuación se introducen las soluciones que una PN debe proporcionar para dar respuesta a las necesidades del usuario.

Llegados a este punto, la primera tarea a emprender consiste en especificar la manera de gestionar los diversos servicios en una PN. Pero antes de poder determinar las características de la plataforma que los gestione, hay que conocer el ciclo de vida de un servicio. El ciclo de vida de un servicio se define como la colección de estados en los que éste se puede encontrar desde que se crea hasta que se destruye e incluye todas aquellas operaciones que se llevan a cabo con él en cada uno de esos estados y que pueden provocar la transición hacia otro estado diferente. Un servicio se crea como respuesta a una necesidad concreta en un momento dado. El creador puede basarse en plantillas o patrones existentes o bien realizar el desarrollo desde cero. Esta fase implica la descripción del servicio y la definición de su lógica de funcionamiento y de la interfaz de interacción. Posteriormente, el creador debe dar a conocer el servicio; para ello publica su descripción en un directorio de servicios. Será a partir de entonces cuando ese servicio esté disponible para su uso. Mediante herramientas de búsqueda cualquier usuario puede descubrir el servicio (si se ajusta a sus necesidades) y solicitar su provisión y/o ejecución, iniciándose una sesión de servicio. Toda vez que el servicio ha cumplido su propósito, esta sesión se finaliza y se da por concluido el ciclo de vida del servicio.

A la vista de lo anterior, la plataforma de gestión de servicios dentro de la PN tendrá que dar soporte a la creación, descubrimiento y provisión de servicios en el entorno de la PN de una forma transparente y coordinada. Además de permitir el acceso a servicios personales de forma interna, la plataforma también debe tener en cuenta la existencia de servicios externos. A todo esto hay que añadir que, del mismo modo que las capas inferiores de la PN soportan heterogeneidad (en dispositivos, en tecnologías radio inalámbricas, etc.), a nivel de servicio también se debe permitir la integración de servicios desarrollados u ofrecidos con diferentes metodologías y plataformas.



Figura 3.21: Capa de Abstracción a Nivel de Servicio

La Capa de Abstracción a Nivel de Servicio de una PN (figura 3.21) aúna los mecanismos y protocolos necesarios para cumplimentar los requerimientos descritos. Se define la plata-

forma de gestión de servicios (SMP, *Service Management Platform*) como un entorno de servicio modular y escalable que se ajusta a las necesidades de la P-PAN y la PN. La idea se origina en el ámbito del proyecto MAGNET, pero el trabajo de esta tesis ha evolucionado el concepto.

La SMP plantea una arquitectura orientada a componentes, tanto desde el punto de las entidades funcionales que la componen como de los propios servicios. De una parte, las funcionalidades previstas pueden implantarse en un único nodo o, siguiendo la creciente tendencia a la disgregación, pueden distribuirse entre varios. Por otro lado, los servicios se sustentan de la forma más descentralizada y modular posible a partir del conjunto de componentes que residirán en diferentes nodos. El uso de componentes de servicio posibilita un mayor grado de personalización, ya que dejan de ser entidades monolíticas invariantes para convertirse en algo dinámico y adaptable en cada momento a lo que el usuario reclame.

3.6.1. Conceptos previos

Antes de profundizar en la descripción de la arquitectura funcional de servicios de una PN es necesario presentar y definir a modo de introducción los principales conceptos que se manejan en relación a ellos:

- **Componente:** Un componente es una entidad *software* que ofrece una funcionalidad básica, que en cooperación con las ofrecidas por otros componentes o de forma autónoma habilita la provisión de un servicio final al usuario. Todo componente puede ser sensible al contexto.
- **Servicio:** Un servicio es una entidad *software* compleja, concebida a partir de uno o varios componentes, sensible al contexto, que se ejecuta en la red (p. ej. la PN) o en un nodo personal, y proporciona valor al usuario.
- **Composición:** Procedimiento por el cual se seleccionan y se organizan los componentes que mejor se adaptan a las necesidades y expectativas del usuario en un momento dado para proveer un determinado servicio. Según la forma en que se relacionan los componentes existen distintos modelos de composición entre los que destacan las estrategias de coordinación, cableado, orquestación y coreografía de servicios [21, 121]. Es importante reseñar que un servicio podrá estar formado por la interacción de varios servicios, que actuarán como componentes atómicos dentro del servicio compuesto.
- **Plantilla de servicio:** Descripción estática de un servicio que incluye toda la información relativa a éste que se va a necesitar a lo largo de su ciclo de vida. Una plantilla se compone de un bloque de información básica (ID del servicio, creador, etc.), un bloque de lógica (secuencia de composición y/o orquestación), un bloque de semántica (descripción del servicio para permitir su descubrimiento) y un bloque de seguridad (listas de control de acceso, información de autenticación, autorización y compensación (AAA, *Authentication, Authorization and Accounting*), etc.). El uso de plantillas facilita la reutilización y extensibilidad de los servicios.
- **Contexto de servicio:** aquella información o circunstancias que son de utilidad durante el proceso de composición de los servicios, como la disponibilidad de un determinado componente o su adecuación al usuario que lo ha solicitado.

3.6.2. Descripción de alto nivel

En la figura 3.22 se representa la arquitectura de servicios planteada para dar respuesta a las necesidades surgidas en la PN.

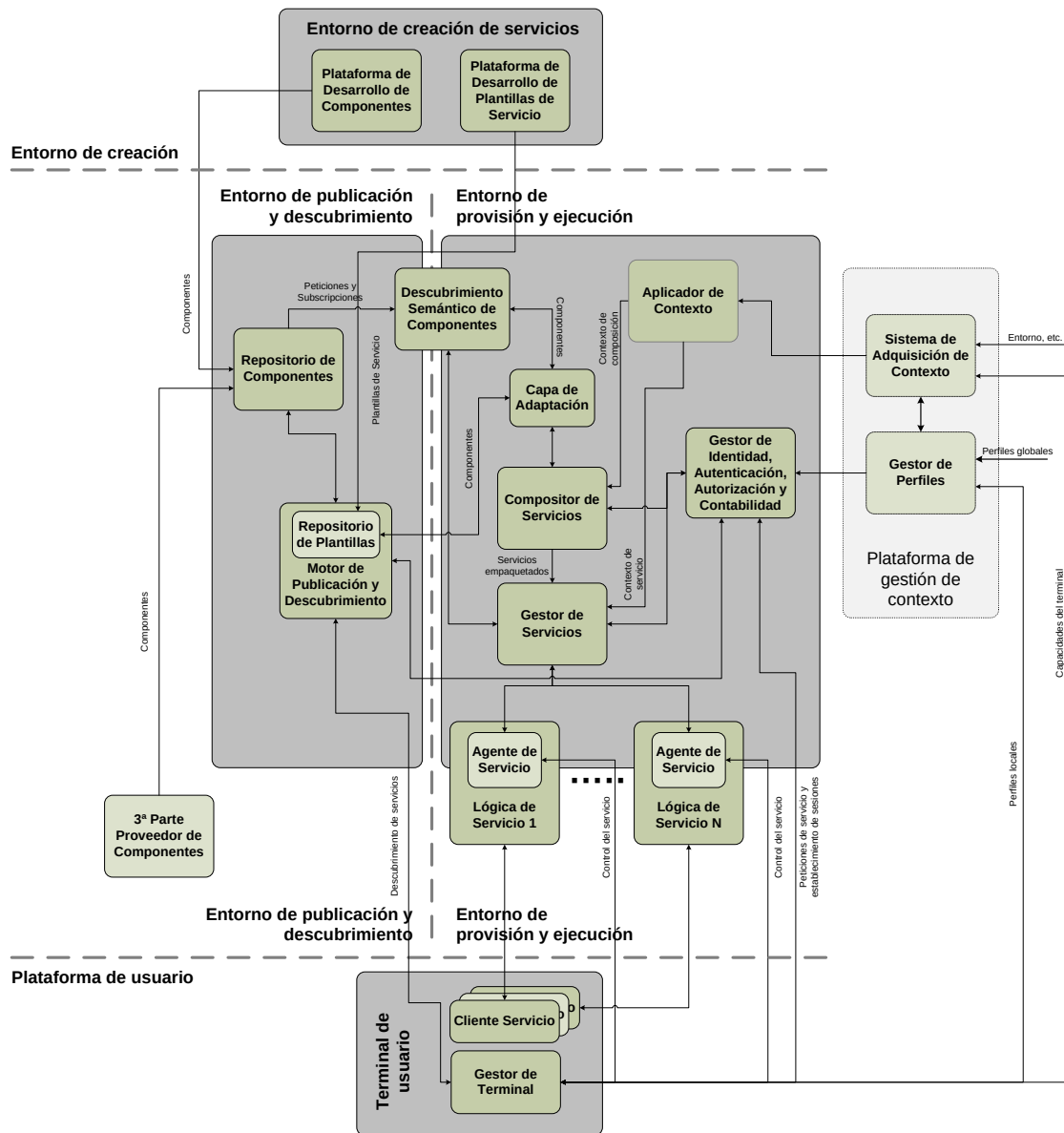


Figura 3.22: Arquitectura de la plataforma de gestión de servicios

Se pueden diferenciar cuatro grandes dominios funcionales:

- Entorno de creación: donde se concentra la fase de diseño del servicio.
- Entorno de publicación y descubrimiento: donde se anuncia el servicio para su distribución y se establecen los mecanismos de búsqueda en los directorios de servicios.

- Entorno de provisión y ejecución: donde se gestiona la sesión de uso del servicio seleccionado por el usuario.
- Plataforma de usuario: donde se proporcionan las funcionalidades más allá de la mera lógica del cliente del servicio, de forma que la provisión sea personalizada en todo momento.

Como dominio adicional transversal a toda la PN ya se ha indicado que existe la Capa de Abstracción a Nivel de Contexto. En este sentido existe un módulo de enlace entre la SMP y la plataforma de gestión segura del contexto (SCMF, *Secure Context Management Framework*), el Aplicador de Contexto (AC), que ofrece la interfaz para adaptar los servicios al perfil y entorno del usuario.

La seguridad dentro de la PN se establece y se garantiza mediante la relación de confianza existente entre los nodos de la PN. Los problemas pueden originarse por la apertura de la PN a nodos externos, bien para usar servicios ofrecidos fuera de la PN o bien porque el usuario permita el uso de sus servicios a esos nodos externos. El acceso y ejecución de los servicios se realiza a través de un grupo funcional genérico que actúa como Gestor de Identidad, Autenticación, Autorización y Compensación (GIAAC), todo ello siguiendo las bases de seguridad planteadas dentro de la PN. Además de identificar a los usuarios durante el descubrimiento y el acceso al servicio mediante el uso de soluciones como duplas usuario/clave, pertenencia a grupos o sesiones basadas en *Transport Layer Security* (TLS), etc., este módulo añade un componente AAA con capacidades para facturación y pago de los servicios provistos. Si bien este concepto no se ha explotado, las descripciones incluidas en el documento Open Mobile Alliance (OMA) *Best Practices* [122] deberían ser tenidas en cuenta en el desarrollo de nuevas funcionalidades para la PN.

3.6.3. Entorno de creación

Un servicio se ha definido como una agrupación ordenada de componentes. Por tanto el proceso de creación de un servicio se supedita a la creación de los componentes que lo componen y a determinar cómo se relacionan entre ellos.

El dominio funcional de creación de servicios concentra las etapas de diseño y generación *offline* de los servicios por parte del usuario o de los proveedores de servicios externos, de confianza o no. Básicamente se compone de dos bloques funcionales, el primero centrado en el desarrollo de componentes de servicio, mientras que el otro consiste en definir la interacción de esos componentes bajo unas reglas definidas a través de plantillas.

La funcionalidad de un componente puede estar vinculada a las capacidades de un nodo o ser independiente de éste. Los componentes definidos incluirán, junto con sus interfaces, información semántica en la sección de metadatos, las posibilidades de configuración y adaptación al contexto, etc. En la figura 3.23 se representa la estructura interna de un componente de servicio.

El servicio en si se define a través de las plantillas. Una plantilla de un servicio define el conjunto mínimo de componentes para ofrecer una funcionalidad básica, aunque también puede incluir opciones que proporcionen una experiencia de valor añadido. Si bien la plantilla no predefine qué componentes formarán parte del servicio cuando que éste se sirva a un

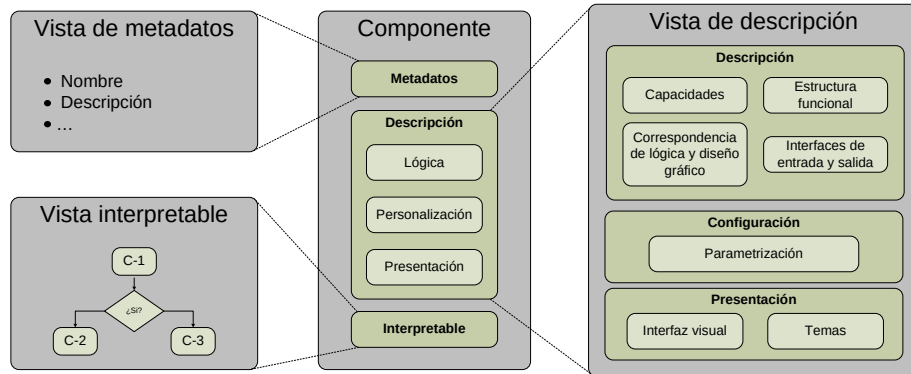


Figura 3.23: Detalle de un componente de servicio

usuario final, sí que define las funcionalidades que se ofrecerán en último término al usuario y los pasos intermedios para lograrlo. En este sentido, las plantillas estarán compuestas por descripciones semánticas de las funcionalidades, de forma que se facilite el proceso de búsqueda y de composición dinámica a partir de los componentes disponibles y el contexto del usuario.

Más allá de la información que apoye a la generación del servicio, las plantillas incluirán datos que faciliten el descubrimiento e información sobre la manera de invocar el servicio por parte del usuario.

De forma general, se puede considerar que una plantilla de servicio tiene un formato similar a la de un componente, pero que adicionalmente incluye la lógica del servicio, es decir, la forma en que los componentes se organizan y relacionan.

Un inconveniente que se puede atribuir a esta aproximación al servicio es la complejidad que el proceso de composición involucra. No será la funcionalidad ofrecida el aspecto en el que el usuario tendrá que hacer mayor hincapié a la hora de crear cada componente, sino en las interfaces que éstos ofrecen tanto para desarrollar la propia lógica del servicio como para permitir una gestión de su ciclo de vida. Por esta razón, la plataforma de desarrollo de componentes incluye una herramienta de verificación de la consistencia de esas interfaces, buscando que todos los componentes sean lo más homogéneos posible.

3.6.4. Entorno de publicación y descubrimiento

Dada la gran variedad de servicios que una PN puede ofrecer y la multitud de dispositivos y nodos donde pueden ser accesibles, la SMP emplea una metodología multinivel para hacer frente a la publicación y búsqueda de los servicios [20]. En este sentido, el procedimiento jerárquico seguido se extiende a partir de la organización natural de la PN, como se ilustra en la figura 3.24, diferenciándose 5 niveles: DR, P-PAN, *cluster*, PN y global.

Los procesos de descubrimiento son asistidos por dos entidades:

- El SMN, es el nodo responsable de las tareas de descubrimiento dentro de cada uno de los niveles definidos. Se recomienda que los SMN sean aquellos nodos con más capacidades dentro del *cluster*.

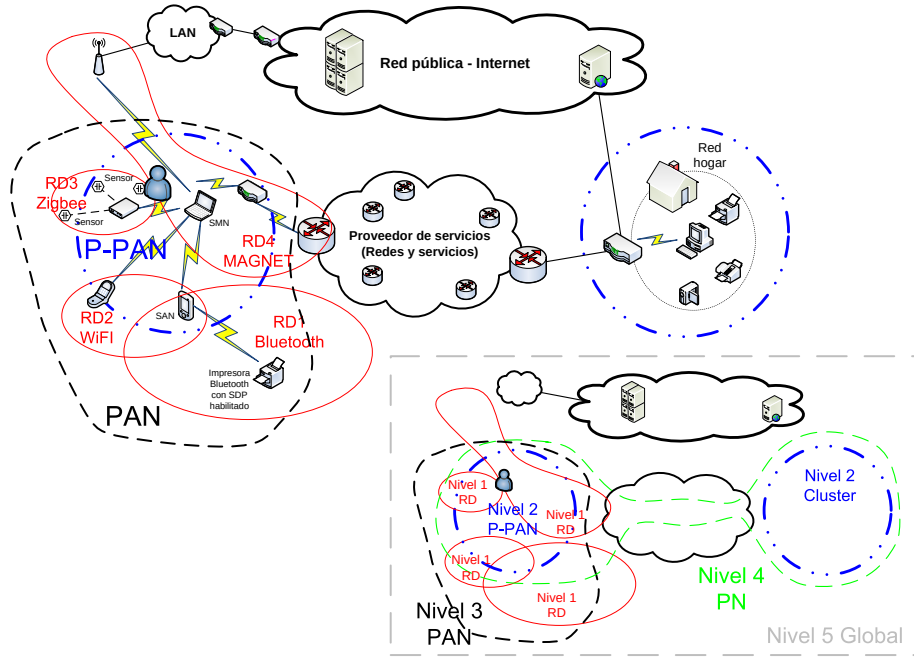


Figura 3.24: Paradigma de gestión de servicios multinivel

- El nodo asistente en la gestión de servicios (SAN, *Service Assistance Node*), es un nodo que por sus capacidades es capaz de ejecutar las tareas del SMN. Los SAN son los nodos que participan en el proceso de contienda que erige a uno de ellos como SMN.

En cada *cluster* existe un único SMN. A través de un procedimiento de contienda entre los SAN, donde el potencial de cada uno se calcula ponderando diferentes métricas relacionadas con las características del nodo (batería, potencia de cómputo y almacenajes, comunicaciones, funcionalidades SMP disponibles, etc.), se selecciona el nodo más adecuado para tomar el rol de SMN [20, 123]. Cuando un SAN reemplaza a un SMN, como parte del traspaso de funciones, se intercambian información de los servicios ya descubiertos o provistos. Por supuesto este traspaso amigable es sólo posible cuando el reemplazo se realiza debido a que las capacidades del SMN han disminuido y no puede ejercer sus tareas de una forma eficiente. En cualquier otra situación, el nuevo SMN tendrá que iniciar su labor desde cero.

En lo concerniente a la gestión de los servicios, los niveles 1, 2 y 3 siguen un enfoque centralizado, siendo los SMN quienes descubren los servicios disponibles en su circunscripción. Una vez que tanto la descripción de los componentes como la plantilla de servicio está disponible, el SMN deberá ser capaz de localizarla e incluirla en su base de datos. No obstante, para facilitar la tarea, el usuario, como gestor de su PN, puede invocar el proceso de publicación de forma manual.

En el resto de los niveles, los SMN de la PN intercambian la información de servicio distribuida en la PN a través de una red P2P, similar a la representada en la figura 3.25. El paradigma P2P, en contraposición al tradicional modelo cliente-servidor, permite que los nodos compartan sus recursos de forma directa, con un uso residual o inexistente de servi-

dores centrales. Esto permite acelerar los procedimientos de búsqueda al alojar localmente parte de la información de localización de los servicios [124]. Dado que existen múltiples opciones para dar soporte a una red P2P, la PN no impone una solución. Típicamente durante los trabajos realizados en esta tesis, dentro del marco del proyecto MAGNET, se han empleado JXTA [125] e INS [126], aunque cualquier otra hubiera sido igualmente válida.

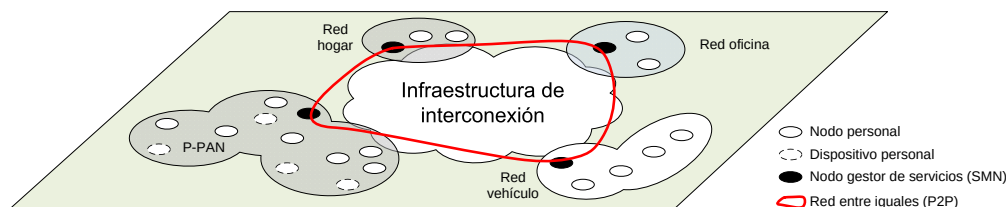


Figura 3.25: Red distribuida de intercambio entre SMN

Siguiendo la aproximación jerárquica, si una búsqueda resulta infructuosa dentro del *cluster*, el SMN redirigirá dicha petición a sus homólogos dentro de la red superpuesta de servicios, quienes, si conocen el servicio, responderán. La interacción entre los nodos SMN dentro de la SMP sigue los requerimientos de seguridad y privacidad impuestos por la PN, donde aplican las soluciones planteadas a nivel de conectividad y de red.

Las tareas de descubrimiento de servicios están estrechamente ligadas con la publicación. Los SMN ejecutan también directorios de servicios que permitirán al usuario listar los servicios y componentes disponibles en la PN. Este es el paso previo a seleccionar, mediante procesos de búsqueda semántica, el servicio más adecuado a las necesidades y proceder a su provisión.

Una vez se han descrito las entidades y la metodología que se emplean en el descubrimiento y publicación de los servicios, a continuación se establece la relación entre los componentes funcionales que conforman la SMP y que se ejecutan en el SMN. Limitando las capacidades de la PN, no es obligatorio que todos los módulos estén disponibles en el SMN.

El paso necesario para que todo servicio pueda ser consumido es lograr que el usuario conozca la existencia de ese servicio y sus características. Dentro de una PN el usuario conocerá los servicios propios definidos por él, pero lo más probable es que no recuerde ni su localización, ni interfaces, ni características detalladas. El Motor de Publicación y Descubrimiento (MPD) sirve de portavoz informativo de los servicios disponibles. Este bloque funcional almacena las plantillas descubiertas, así como los componentes o vínculos directos a ellos, de forma que pueda responder de manera efectiva con la funcionalidad requerida a las peticiones del usuario. Cuando un usuario inicie la búsqueda de un servicio con la semántica asociada, el MPD devolverá los detalles de cómo crear una instancia de un servicio que responda a sus necesidades.

El vínculo entre el MPD y el Coordinador Radio (CR) es, por tanto, muy fuerte, ya que las respuestas a las peticiones de usuario contendrán los enlaces a un subconjunto de potenciales componentes de servicio, cuya composición proporcione el servicio solicitado. Para facilitar la tarea de descubrimiento de componentes el CR categoriza su contenido, agrupando los componentes según la funcionalidad que provean. La idea subyacente tras el

concepto de categorización no se restringe a permitir un acceso más rápido a las posibilidades de implementación de un servicio, sino que busca que dos componentes cualesquiera de una misma categoría puedan ser reemplazados sin que la operativa del servicio se vea afectada.

Es aquí donde juega un papel muy importante la información proporcionada en los metadatos de los componentes. La Capa de Adaptación de Servicio (CAS) se concibe como una capa de convergencia que aporta el soporte a la heterogeneidad en términos de servicio. Existen muchas y muy diversas formas de crear, describir y ejecutar servicios y componentes. De igual forma que la UCL oculta la diversidad en las interfaces de comunicaciones, la CAS proporciona los medios para no sólo soportar múltiples tecnologías de servicio y sus interfaces dentro de la SMP, como por ejemplo *Universal Plug and Play* (UPnP), *Simple Object Access Protocol* (SOAP), Bluetooth, *Service Location Protocol* (SLP), etc., sino también permitir que cualquier miembro de la PN pueda relacionarse con el SMN en diversos lenguajes. Cabe mencionar que ese soporte incluye la interacción entre los SMN dentro de su red P2P de servicio.

3.6.5. Entorno de provisión y ejecución

Validada y autorizada la petición de servicio de usuario, llega el momento de proveerlo. El SMN es el encargado de seleccionar los componentes más adecuados de entre los disponibles según el contexto que involucre la ejecución del servicio. El Compositor de Servicios (CS) residente en el SMN toma toda la información disponible del contexto y de la plantilla seleccionada y trata de confeccionar el servicio más óptimo.

Ya se ha comentado que los componentes pueden ser de muy diversa naturaleza. La categorización dependiendo de su funcionalidad reduce notablemente la tarea de selección de los componentes. En este sentido, los componentes de una misma categoría deberían ser intercambiables. Pero de la misma forma que se da la diversidad en la funcionalidad, también existe en la forma de implementarlos y las interfaces que exportan. Nuevamente la CAS envuelve las divergencias entre las interfaces de forma que los componentes se puedan interconectar tal como se indique en la plantilla del servicio. No obstante, las interfaces de entrada y salida de los componentes deben ser concebidas de la forma más universal posible. Incluso componentes confeccionados sobre tecnologías similares serán más propensos de ser combinados en el servicio final, pues se reduce la carga computacional dado que los componentes provistos desde el mismo nodo podrán compartir la misma instancia del mismo motor de ejecución. La figura 3.26 ejemplifica cómo a partir de dos componentes, uno que proporciona la posición a través del *Global Positioning System* (GPS) y otro, p. ej. un sistema de información geográfica (GIS, *Geographic Information System*), que la toma como entrada se crea un servicio de localización.

Una vez que las instancias de los componentes de servicio han sido integradas, el usuario puede ejecutar y disfrutar de un servicio personalizado. No obstante, ya se ha insistido en que la movilidad es una de las características intrínsecas de la PN. En movilidad será necesario monitorizar y gestionar el servicio para adaptarlo a las nuevas situaciones que su consumidor se vaya encontrando. Las cuestiones de conectividad han sido solventadas en la Capa de Abstracción de Nivel de Red y el direccionamiento seleccionado facilita la gestión de la movilidad. A pesar de ello no hay que olvidar mantener la monitorización del servicio

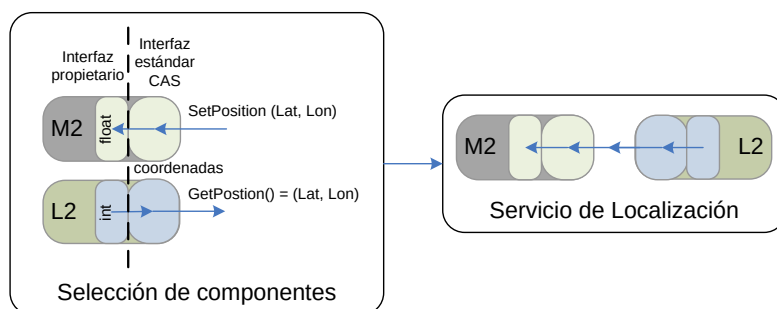


Figura 3.26: Ejemplo de composición de servicios a partir de componentes

para actuar con celeridad ante situaciones imprevistas y mantener la QoS y la QoE. El SMN es el integrador del servicio y, por tanto, se erige en la entidad más adecuada para actuar como gestor de la sesión (ver figura 3.27), tarea que se realiza a través del Gestor de Servicios (GS). Actuando como intermediario, monitorizando y controlando la operativa del servicio, con el consentimiento del usuario, tomará decisiones sobre el ajuste o cambio de componentes, etc. El conocimiento que el SMN y su GS tienen de los componentes y servicios disponibles hace que puedan manejar de forma fluida cualquier situación extraordinaria que se pueda dar.

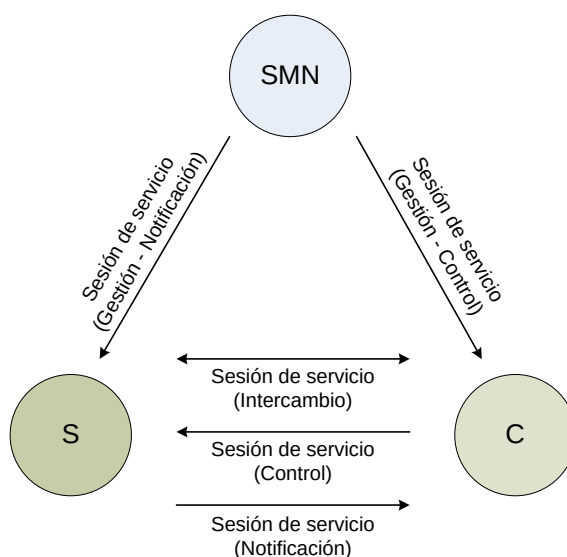


Figura 3.27: Gestión de la sesión de servicio

El GS, una vez compuesto el servicio, añade un componente adicional denominado Agente de Servicio (AdS) que monitoriza la ejecución y sirve de enlace para informar de las eventualidades que surjan.

El traspaso de sesiones entre terminales es una de las acciones más complejas de gestionar, ya que en la mayoría de los casos no sólo implica el cambio de dispositivo sino también de las características de éste. La solución más común en esta situación es la recomposición del servicio tratando de emplear aquellos componentes que se ajusten mejor al nuevo dispositivo

donde el usuario consumirá el servicio. Por ejemplo, para el caso de un servicio multimedia que se traspare desde un terminal móvil a una televisión se adaptará el servicio con el uso de componentes que permitan una codificación de mayor calidad, de forma que el visualizador proporcione una mejor QoE.

3.6.6. Plataforma de usuario

El ejemplo anterior sugiere una nueva necesidad: parte de los servicios, e incluso de la gestión de estos, en la mayoría de los casos no se puede ejecutar totalmente de forma remota en entidades residentes en la PN. Existen funcionalidades que son dependientes del terminal a través del cual el usuario ejecuta el servicio y que deben correr en éste. La respuesta a esta cuestión se obtiene mediante lo que se ha denominado como entorno de plataforma de usuario.

El cliente de ejecución de un servicio, aunque basado en tecnologías lo más estándar posible, normalmente tiene que emplear recursos disponibles y ejecutables en el terminal de usuario. El empleo de navegadores web para acceder a los contenidos o para comunicarse con el servicio es un ejemplo.

En ciertas ocasiones, para extender las funcionalidades, se podrán definir componentes que permitan una mejor interacción con las entidades remotas. Dichos componentes serán confiables ya que estarán certificados y serán descargados siguiendo las políticas de seguridad impuestas por la red personal. La descarga de aplicaciones móviles adaptadas al usuario que soporten un entorno de interacción más amigable, incluyendo capacidades adicionales de seguridad, etc. son una muestra de lo que se consideran componentes de servicio localmente ejecutables.

En todos los casos, tanto los componentes locales como aquellos que se ejecuten de forma remota, se adaptan a las características del terminal de usuario y del cliente de ejecución del servicio.

3.6.7. Interacción entre componentes funcionales

En la figura 3.28 se presentan las interrelaciones entre las diferentes entidades que, ejecutándose en el SMN y el terminal de usuario, conforman la operativa de la SMP. La secuencia temporal ordena las fases del procedimiento de descubrimiento, composición y ejecución de los servicios. Se han dejado fuera tanto la creación como la publicación de los servicios, ya que son etapas poco automatizadas y fuertemente guiadas por el usuario, donde la interacción entre componentes se reduce a incluir las diversas descripciones de componentes y servicios en los diferentes repositorios, y por tanto su comprensión es directa.

El proceso descrito se inicia con la voluntad del usuario de descubrir algún servicio o funcionalidad que dé respuesta a sus necesidades. Haciendo uso de la arquitectura definida en las secciones anteriores, obtiene el servicio deseado como la integración de diferentes componentes que debidamente orquestados proporcionan la funcionalidad requerida. A continuación, referenciando la figura 3.28, se desarrolla en mayor profundidad cada una de las interacciones identificadas.

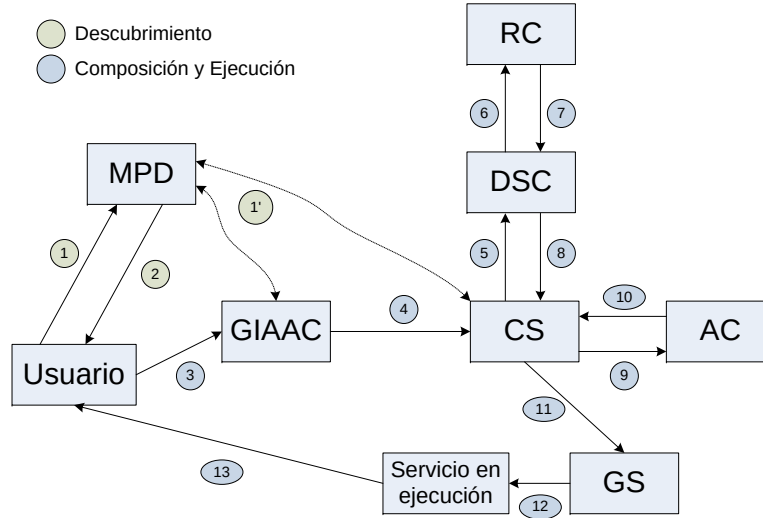


Figura 3.28: Secuencia del descubrimiento, composición y ejecución de servicios

3.6.7.1. Descubrimiento de servicios

El proceso de búsqueda de servicios puede iniciarse de dos maneras: por iniciativa del usuario o de forma automática a instancias del contexto. Mientras que en el primer caso el usuario describirá mediante un lenguaje natural qué servicio busca, en el segundo esa búsqueda será de forma automática a partir de un evento previamente definido (p. ej. localización, etc.). Es en esta fase inicial donde el gestor o aplicación residente en el terminal de usuario haciendo uso de una interfaz universal transmitirá los parámetros de la búsqueda al SMN del *cluster*.

Tomando como base el diagrama de la figura 3.28, la figura 3.29 describe el detalle de la interacción de las diferentes entidades durante la búsqueda de un servicio.

En la petición de búsqueda el usuario incluye los denominados parámetros estáticos, es decir, aquellos que se envían de forma previa al inicio de la ejecución del servicio. Entre ellos se encuentra una descripción semántica del servicio, en lenguaje formal, *Ontology Web Language* (OWL) u otro, e información acerca de las capacidades del terminal, credenciales, entorno, etc. con el objetivo de ajustar lo más posible los resultados al contexto y perfil del usuario.

El mensaje de búsqueda se lanza al SMN del *cluster*, gestionando éste el descubrimiento dentro de la PN (etapa 1 de la figura 3.29). El SMN, ante la imposibilidad de responder a la petición del usuario, redirige la solicitud al resto de los SMN de la PN a través de la red superpuesta de servicio. Será el MPD el encargado de esta acción. El MPD previamente solicita al GIAAC que compruebe si la identidad y las credenciales aportadas son válidas (etapa 2 de la figura 3.29). Con el visto bueno del GIAAC se procede a la búsqueda de todos aquellos servicios disponibles que se ajusten a los parámetros recibidos (etapa 3 de la figura 3.29).

Según la lista de servicios candidatos obtenida (etapa 4 de la figura 3.29), el SMN analiza las diferentes combinaciones de componentes que puedan completar y dar soporte a las

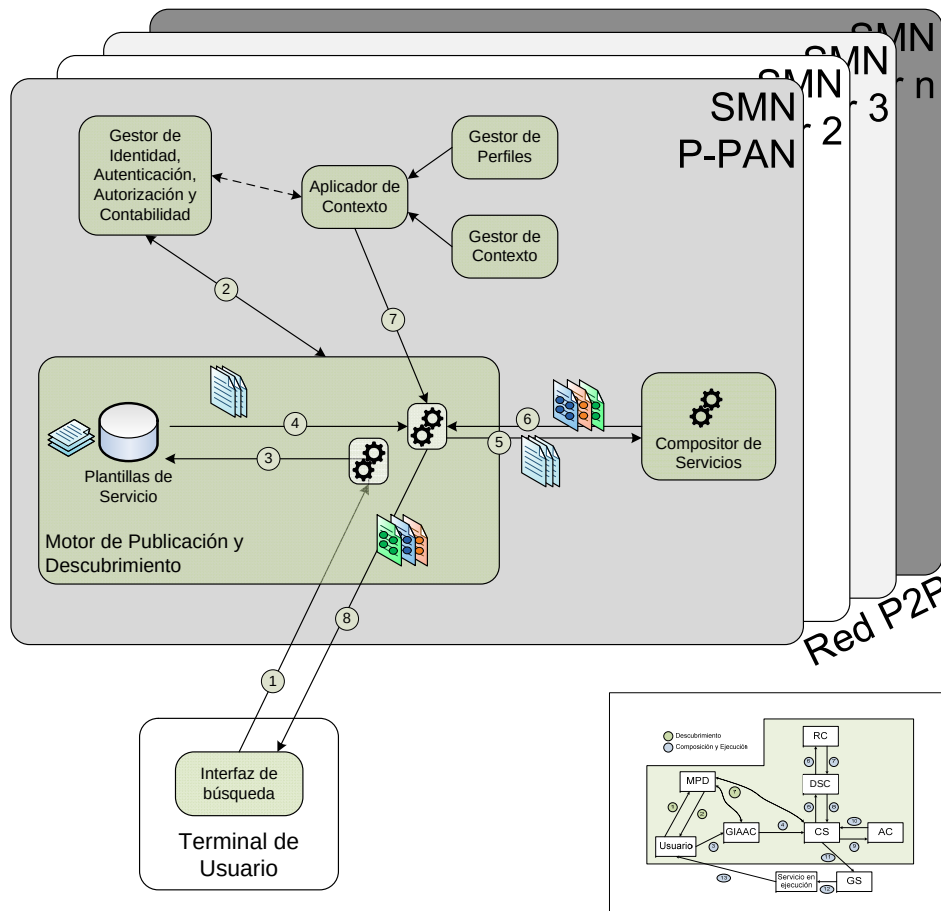


Figura 3.29: Detalle de interacciones entre componentes para el descubrimiento y selección de un servicio

plantillas de los diferentes servicios. El CS obtiene la plantilla de los servicios que van a ser ofertados (etapa 5 de la figura 3.29) y busca en los CR aquellos que mejor se ajusten a los parámetros recibidos (etapa 6 de la figura 3.29). Este listado, junto con la información proveniente del AC (etapa 7 de la figura 3.29), es filtrado y ordenado con el fin de retornar al usuario o terminal un resultado lo más ajustado posible (etapa 8 de la figura 3.29). Reseñar que en este punto no se ha realizado la orquestación de los diferentes componentes que resulte en su ejecución, sino que únicamente se han rellenado los huecos de la plantilla del servicio empleando los componentes disponibles. Los diferentes componentes se encuentran únicamente enumerados pero no conexonados entre sí para producir el servicio final, es decir, sus interfaces no han sido conectados. Esta tarea se realizará únicamente cuando se realice la composición del servicio escogido para su ejecución.

El agente de servicios en el terminal muestra la lista ordenada al usuario, tras lo cual el usuario realiza la selección que dará lugar a la ejecución final de un servicio. Algunos de los servicios enumerados pueden ofrecer demostraciones de su operativa para facilitar la decisión final. Estos casos son conocidos como descubrimiento con estimación de resultados, bien a través de una ejecución gratuita con capacidades restringidas o bien ofreciendo ejemplos

predefinidos. Estas situaciones llevan a la composición real del servicio en ejecución y, por tanto, las diferentes pruebas implicarán que todo el proceso descrito a continuación sea completado.

Una vez seleccionado un servicio, éste se guarda dentro del contexto de usuario como servicio preferido, último en usarse o una etiqueta similar, de forma que en futuras búsquedas el contexto pueda priorizar este resultado.

3.6.7.2. Composición y ejecución de servicios

A partir de las plantillas obtenidas, la composición y posterior ejecución se realiza creando instancias de los componentes que formalicen el servicio. La figura 3.30 representa el detalle de la interacción para la creación de un servicio, ejemplificado para el caso de un servicio de localización.

En primer lugar, el CS solicita los componentes dentro de las categorías que se necesitan para el rellenar la plantilla del servicio seleccionada (paso 5 de la figura 3.30). En la figura 3.30 se muestran como ejemplo los componentes de mapas y posicionamiento. Aquellos componentes que respondan a las necesidades son analizados por la CAS para normalizar las interfaces (etapas 6 y 7 de la figura 3.30). El CS, con ayuda bien del contexto del usuario o bien del propio usuario (etapas 8, 9 y 10 de la figura 3.30), selecciona los componentes específicos que se ajusten mejor a las necesidades del usuario y compone el servicio final. Para el caso del servicio de localización usado como ejemplo, el usuario necesita la posición en la que se encuentra y representarla en un mapa. Así, la entrada del componente mapa se vincula a la salida del componente posicionamiento. En ese momento, ambos interfaces son ya compatibles.

A partir de entonces el servicio empaquetado es gestionado por el SMN, quien se encargará del resto del ciclo vital del servicio en ejecución mediante el AdS específico, delegando aquellas funcionalidades que deban ser ejecutadas en el entorno del usuario a la plataforma de usuario (etapas 11 y 12 de la figura 3.30).

Una vez que los diferentes componentes estén emplazados en el lugar que les corresponde y se hayan establecido estas nuevas interrelaciones, el servicio pasa a su estado de ejecución (etapa 13 de la figura 3.30). Los cambios en el contexto durante la ejecución del servicio o los producidos a instancias del propio usuario o del mismo servicio en ejecución pueden motivar modificaciones en la composición del servicio, desencadenando nuevas búsquedas semánticas de componentes. El SMN con el AdS serán las entidades que gestionarán esa información. Por tanto, en el caso de que se produzca esa situación y alguno de los componentes que cambien hayan sido enviados previamente al terminal, deberán eliminarse del mismo y ser sustituidos por aquellos fruto de la nueva búsqueda. Es necesario que este proceso se realice de la forma más transparente posible para el usuario, sin que la lógica ni el estado del servicio se vean afectados.

La ejecución de un servicio dentro de la PN por parte del usuario no debería acarrear ningún gasto para el usuario pues en la mayoría de las ocasiones se trata de servicios propios. No obstante, en el caso de ofertar servicios a usuarios externos, el GIAAC no solo se ocupará de velar por la seguridad de la PN sino que además será el encargado de realizar los cargos pertinentes.

de uso. Para ello la filosofía de diseño y provisión de los servicios debe modificarse y hacer que éstos sean conscientes de los objetos y usuarios que rodean a sus consumidores. En el ámbito de la PN se ha dado un primer paso en este sentido, tal y como se ha descrito en las secciones anteriores, con la definición de un entorno de servicios dinámico, adaptable y centrado en el usuario.

No obstante, aún queda por plantear la metodología que se empleará en la gestión de la información del entorno inteligente que surtirá a los servicios de usuario. No sólo habrá que considerar la adaptación de las interfaces de usuario o la operativa de los servicios al contexto, sino también la recolección de datos, su almacenamiento y compartición. Más importante aún es dar solución a las necesidades de razonamiento en aras de procesar los datos y proporcionar un valor añadido. Todo esto hará realidad el concepto de PN totalmente consciente del usuario y su ecosistema.

Antes de tratar de definir una plataforma que gestione el contexto de forma inteligente y ordenada, es necesario concretar el significado de contexto. Se trata de un concepto empleado de diversas maneras [127-129] y todas ellas lo relacionan con el conjunto de información que describe la situación de una entidad física o virtual. Tomando al pie de la letra esta descripción, el contexto es algo infinito. Mas la información relevante para el estado de la entidad es finita, lo que permite limitar el volumen de información a considerar como contexto. La definición globalmente aceptada de contexto y tomada en esta tesis es [130]²:

Contexto es cualquier información que puede ser empleada para caracterizar el entorno de una entidad. Se considera una entidad a una persona, lugar u objeto que pueda influir de manera relevante entre un usuario y una aplicación, incluyendo ambas.

Asumiendo que el contexto es en sí mismo información, resulta adecuado conocer cómo el usuario, sus dispositivos y sus aplicaciones pueden usar esa información. Las metodologías de uso se pueden agrupar según cuatro patrones [131], tal como se muestra en la figura 3.31:

- Contexto como información adicional.
- Contexto como factor modificador del sistema.
- Contexto como retroalimentación.
- Contexto como generador de eventos.

La mayoría de las aplicaciones que han incluido adaptación al contexto en algunos de estos términos se basan en soluciones propias donde el reúso de los componentes funcionales es nulo o prácticamente imposible [132]. Las propuestas basadas en un *middleware* consiguen cierta independencia de la aplicación y permiten compartir la información de contexto entre

²Originalmente en inglés: *Context is any information that can be used to characterise the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves.*

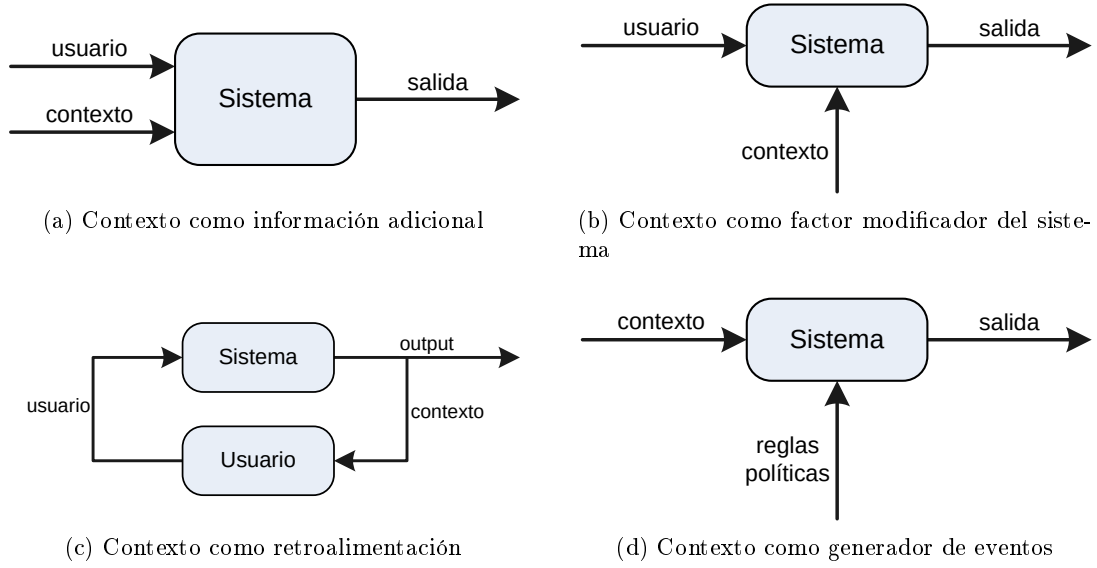


Figura 3.31: Usos de la información de contexto

diferentes entornos [133, 134]. Sin embargo, muchas de estas arquitecturas no se ajustan a la PN al ser mayoritariamente propuestas centralizadas. Si la PN es por naturaleza una red de usuario distribuida, el contexto del usuario en esa red debiera serlo también y así tendrá que ser tratado.

La SCMF es la plataforma dentro de la PN que proporciona las funcionalidades de descubrimiento, mantenimiento, procesado y distribución de la información de contexto. La Capa de Abstracción a Nivel de Contexto se presenta como una capa transversal a todas las anteriores, tal como se muestra en la figura 3.4. Por lo tanto la plataforma en ella desplegada actúa a todos los niveles, tanto recolectando datos como proveyendo información de valor añadido, unificando la forma en la que se trata el contexto dentro de la PN.

El concepto de SCMF, ilustrado en la figura 3.32, se muestra como una capa intermedia entre las fuentes de contexto y los componentes consumidores de esa información. En la SCMF, considerando todo el entorno de la PN, se realiza el almacenaje, intercambio y procesado de la información de forma transparente y segura para el usuario. Aloja además los perfiles y políticas definidas por el propio usuario que se aplicarán a la hora de procesar la información para personalizarla más si cabe.

La información de contexto de un usuario y el perfil con sus preferencias es probablemente la información más sensible relacionada con el usuario. Si dentro de la PN se aplican unas reglas de privacidad, buscando garantizar la integridad y confidencialidad de los intercambios de datos, la SCMF no es la excepción y la seguridad debe ser considerada en cada una de las tareas que ejecute.

La SCMF soporta una gran responsabilidad dentro de la PN, pues gracias a la información que de ella se obtiene se logra en gran medida la personalización de los servicios y las mejoras en el comportamiento de la red. Por esta razón toda su operativa no puede recaer en una infraestructura dedicada, sino que debe adaptarse a la cambiante disponibilidad de

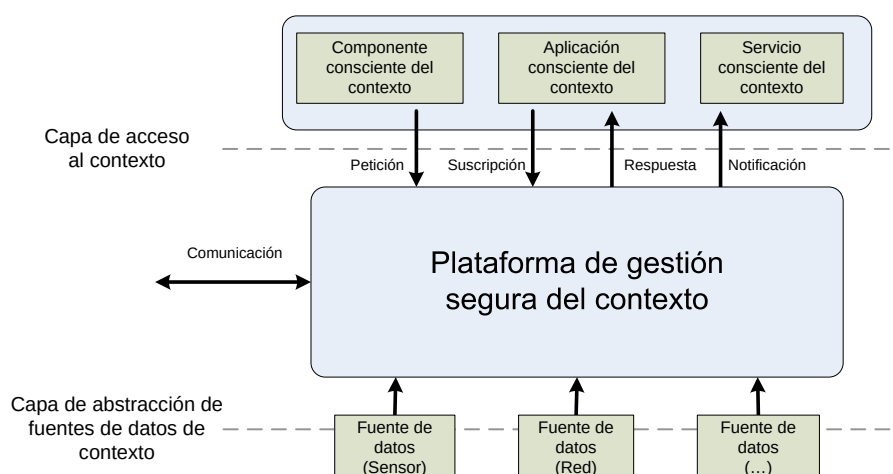


Figura 3.32: Visión global de la plataforma de gestión segura del contexto

nodos y funcionalidades dentro de la PN. Por tanto, tratando de minimizar estos efectos, las funcionalidades de la SCMF deberían ejecutarse en todos los nodos en parte o en su totalidad, haciendo así que la SCMF sea una plataforma distribuida. De esta forma, la colaboración entre todos los nodos de la PN hará viable la disponibilidad del contexto. Se define la entidad Agente de Contexto como aquella que aglutina todas las funcionalidades.

A continuación se describe la arquitectura de alto nivel del agente de contexto, desglosando los múltiples bloques funcionales, para posteriormente proceder a analizar la interacción entre ellos y sus interfaces.

3.7.1. Descripción de alto nivel

La figura 3.33 presenta la arquitectura de alto nivel del agente de contexto. El corazón del agente reside en el gestor de acceso al contexto (CAM, *Context Access Manager*), el módulo de almacenamiento, razonamiento y procesado (P&S, *Processing and Storage*) y el gestor de seguridad en el contexto (CASM, *Context Aware Security Manager*).

Las fuentes de contexto inyectan información de forma propietaria, tanto en su representación como en las interfaces empleadas. Gracias a la capa de abstracción de fuentes de datos de contexto (DSAL, *Data Source Abstraction Layer*) se logra traducir los datos en bruto a una representación común empleada dentro de la SCMF. Estos datos, locales y remotos, se almacenan y procesan para generar información de contexto con valor añadido.

Cualquier entidad, servicios, aplicaciones o el propio usuario, accederá a esta información a través de la interfaz de acceso al contexto (CMI, *Context Management Interface*). Previo acceso a la información se requiere la autenticación y autorización por parte del CASM. Dentro de la SCMF, el CAM se encarga de indexar la información disponible y será quien provisione las peticiones lanzadas.

Tras esta breve descripción, seguidamente se profundiza en mayor detalle en cada uno de los componentes.

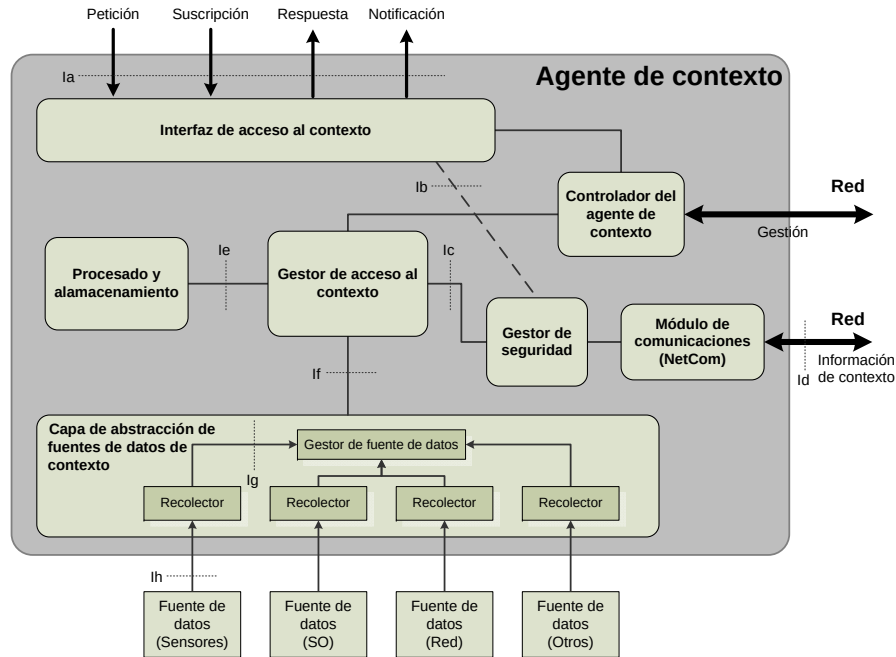


Figura 3.33: Arquitectura de alto nivel de la SCMF

3.7.1.1. Interfaz de acceso al contexto

El CMI es el nexo de unión entre los componentes sensibles al contexto (CACo, *Context Aware Component*) y la SCMF. Los diálogos entre ambos se realizan empleando el lenguaje de acceso al contexto (CALA, *Context Access Language*) [135]. CALA se define como un lenguaje basado en *eXtensible Markup Language* (XML) que facilita la representación del contexto y la definición de acciones sobre él. El CMI realiza la transformación entre este lenguaje de alto nivel y las primitivas internas de comunicación dentro del agente de contexto.

La interacción con el contexto se puede realizar bien de forma síncrona o asíncrona. Se definen dentro de CALA los comandos para implementar estos dos estilos:

- **Petición/Respuesta:** un CACo que necesita puntualmente cierta información de contexto lanza una petición respondida de forma síncrona a través del CMI.
- **Suscripción/Notificación:** un CACo se suscribe a eventos de contexto lanzados por el CMI. Estos eventos pueden ser periódicos, ante un cambio, ante la superación de un nivel de referencia, etc.

El CMI no sólo ofrece interfaces para extraer información, sino que al mismo tiempo incluye los mecanismos necesarios para actualizar cierta información de contexto. En este sentido, a través del análisis de los datos remitidos en las peticiones o suscripciones, el CMI actúa como una fuente de datos de contexto.

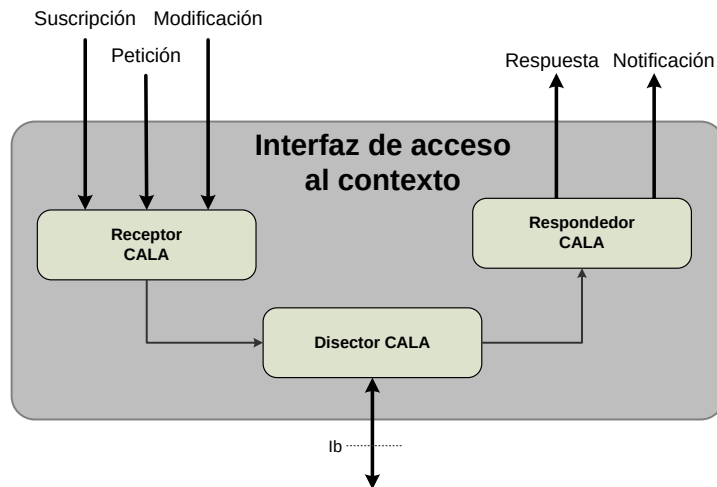


Figura 3.34: Arquitectura del CMI

El CMI se divide en tres subcomponentes tal como se refleja en la figura 3.34: un módulo receptor de peticiones o suscripciones y otro que remite las repuestas o notificaciones generadas en el CALA, ambos ligados a un tercer módulo que realiza la disección y formateo de los mensajes CALA y habilita la interacción con el resto de los módulos del agente de contexto.

3.7.1.2. Controlador del agente de contexto

El controlador del agente de contexto (CAC, *Context Agent Controller*) es el responsable de configurar dinámicamente el agente de contexto. En el arranque del nodo, este módulo se encarga de recoger su configuración base y gestionarla durante todo el ciclo de vida.

La operativa de un nodo puede variar según las funcionalidades que ejecuten sus nodos vecinos. La inclusión de una interfaz de gestión remota en el CAC facilita la coordinación con esos nodos.

3.7.1.3. Gestor de acceso al contexto

El CAM es el módulo que coordina el flujo de información dentro del agente de contexto. Se trata del módulo que debe estar presente en todos los agentes de contexto. Contiene toda la lógica capaz de determinar la fuente de información más adecuada para cumplimentar una petición, de forma que extenderá el ámbito de búsqueda (*local*, *cluster* o PN) dependiendo de las necesidades o incluso podrá seleccionar datos de contexto resultado del procesamiento inteligente de los nativos recibidos de las fuentes. La inclusión del CAM entre el CACo y la información de contexto, permite ocultar el origen de la información.

Admite dos formas de proveer e intercambiar información de contexto (ver figura 3.35):

- Modo valor: el resultado proporcionado es el valor del atributo solicitado. Por ejemplo, en caso de pedir información acerca de lo que está haciendo el usuario, el valor será “en una reunión”.

- Modo referencia: el resultado retornado es un localizador a la entidad que contiene la información. En el ejemplo anterior, la respuesta incluiría un enlace a la agenda personal del usuario, como entidad que aloja la información de estado.

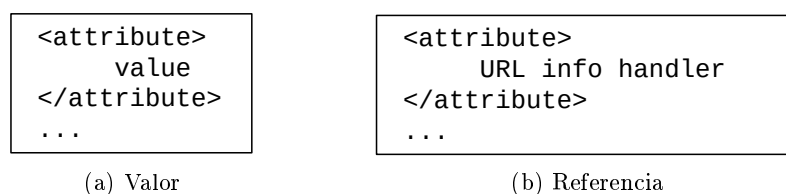


Figura 3.35: Modos de intercambio de la información de contexto

El empleo de una u otra metodología dependerá de las preferencias del usuario. El modo referencia presenta la ventaja de proporcionar un acceso directo a la fuente de información, pero a no ser que se necesite una monitorización constante de la información, se usará por defecto el retorno por valor. Es importante señalar que la validez del localizador vendrá determinada por el CASM, quien tras autenticar y autorizar el acceso a la información, podrá revocar el *token* según las políticas de uso establecidas.

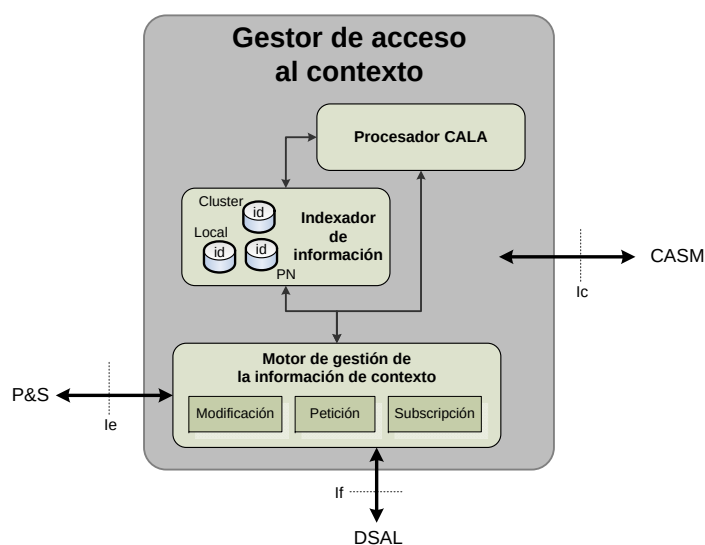


Figura 3.36: Arquitectura del CAM

Tal como se refleja en la figura 3.36, el CAM puede dividirse en tres bloques funcionales: el procesador CALA, el indexador de información y el motor de gestión de la información de contexto. El procesador CALA analiza la petición para configurar su comportamiento interno, p. ej. actualizar las tablas de suscripciones, y gestiona el proceso de envío de las respuestas toda vez que la información solicitada esté disponible. La coordinación con el indexador resulta crucial ya que este último es quien determina dónde están disponibles los datos. Mantiene un listado de la información existente a nivel local, accesible a través de la DSAL o procesada en el P&S, o remotamente en otros nodos.

El motor de gestión de la información de contexto mantiene el enlace con las fuentes de contexto locales. Dado que el flujo de datos de contexto lo atraviesa, emitirá las notificaciones pertinentes en función de los eventos que tenga registrado.

3.7.1.4. Módulo de comunicaciones

La comunicación entre los diferentes agentes de contexto se realiza a través de un módulo dedicado. El módulo de comunicaciones (NetCoM, *Network Communication Module*) es el encargado de empaquetar las primitivas intercambiadas.

Siempre que una consulta no pueda ser resuelta localmente o que un evento deba ser reportado fuera de la entidad donde se haya producido, el CAM solicita al NetCoM que redirija la petición o el comando de gestión. Se recomienda emplear protocolos de transmisión orientados a conexión con el fin de garantizar la recepción y posterior ejecución de las primitivas remitidas.

El NetCoM complementa las propias soluciones de seguridad implementadas en la SCMF empleando los mecanismos de transmisión segura incorporados en los niveles inferiores de la pila de comunicaciones. Buscando el reúso de procedimientos, los mecanismos de seguridad a nivel contexto SCMF pueden mantener una estrecha relación con los ofrecidos a nivel de servicio SMP.

3.7.1.5. Módulo de almacenamiento, razonamiento y procesamiento

Todas aquellas consultas que no pueden ser respondidas directamente a partir de información nativa, requieren de cierta inteligencia y lógica de procesamiento. Por ejemplo, analizar la tendencia de una métrica o las acciones que puede estar realizando un usuario, implican la ejecución de algoritmos sobre los datos básicos. El módulo P&S asume estas tareas. Los datos procesados proporcionados por el P&S son información de contexto, lo que supone que con un cierto nivel de abstracción se puede considerar al P&S como una fuente de datos adicional.

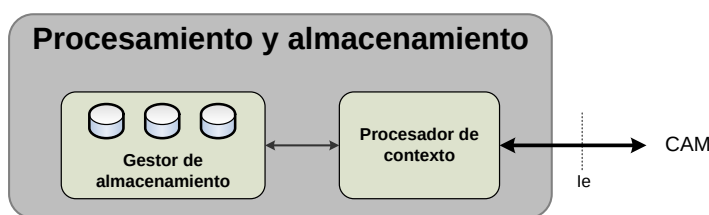


Figura 3.37: Arquitectura del P&S

El P&S no actúa sólo como base de datos donde se almacena la información de contexto y desde la que se da acceso a dicha información a los CACo. El aspecto diferencial con una base de datos tradicional reside en la capacidad de garantizar el uso eficiente de la memoria de almacenaje evitando replicas innecesarias de datos, estimando la validez de los datos guardados, pero sobre todo en el post-procesamiento cognitivo de los datos de contexto para inferir información de valor añadido.

En la figura 3.37 se describe la estructura interna del módulo P&S. El gestor de almacenamiento se encarga de guardar los datos y dotar de acceso a ellos, operando de forma muy similar a una base de datos tradicional. El procesador de contexto se encarga de las tareas de relleno, actualización y control de los datos. Incorpora toda la lógica del motor cognitivo necesario para inferir información de contexto no disponible directamente de otras fuentes de datos. Opcionalmente almacena estos datos para un uso futuro y los emplea para deducir nueva información de contexto. En este sentido, incluye las funcionalidades para evaluar la validez de los datos almacenados, resolver las incoherencias entre datos de diversas fuentes, etc. [136]. Como resultado de estas tareas de gestión, instruirá al CAM con el fin de interrogar a agentes remotos y mantener la consistencia de la información que se genere.

3.7.1.6. Gestor de seguridad

El objetivo del CASM es hacer cumplir las políticas de seguridad impuestas por el usuario con respecto al acceso a su perfil e información contextual. La situación del CASM hace que todo el flujo de información, entrante y saliente, lo atraviese.

Las funciones que realiza el CASM se pueden resumir en:

- Identificación y autenticación de la entidad que solicita la información de servicio (usuario, servicio, etc.).
- Autorización y control de acceso de acuerdo con las políticas.
- Privacidad y confidencialidad de los datos.
- Tarificación (vínculo con SMP).

La SCMF sirve de almacén para el perfil usuario, que incluye entre otros las preferencias y políticas de uso de sus recursos dentro de la PN. Ante cualquier petición que se haga, el CASM instruye al CAM a seguir las premisas impuestas por el usuario. Es por esto que los sistemas incorporados de filtrado de información deben ser suficientemente precisos con el propósito de no revelar datos no deseados. Los perfiles y políticas se guardarán cifrados y firmados para asegurar la confidencialidad y la integridad.

No obstante, toda la seguridad que se implemente dentro de la SCMF no serviría de nada si existiese algún agujero de seguridad en la propia provisión de información. Los canales entre la DSAL y las propias fuentes de datos no deben suponer un riesgo adicional y en la medida de lo posible tienen que satisfacer las premisas de la PN. Por ejemplo, supóngase un servicio que controla la diabetes del usuario. Dicho servicio requiere información biomédica del usuario (niveles de azúcar actuales, lugar donde se encuentra, momento del día, actividad, etc.) para estimar que sus valores de azúcar no caerán por debajo de un cierto nivel. En este caso la información entre las fuentes y la SCMF no debería ser alterada, por lo que el canal de comunicaciones debe asegurar el intercambio.

3.7.1.7. Capa de abstracción de fuentes de datos de contexto

La DSAL es la interfaz que uniformiza el acceso a la información de las diferentes fuentes de datos. Implementa tanto el acceso síncrono mediante petición-respuesta como el asín-

crono mediante el esquema suscripción-notificación de eventos tal como exige la operativa interna de la SCMF. La arquitectura de la DSAL propuesta se muestra en la figura 3.38 y se ha diseñado de forma que permita la integración sencilla de numerosas fuentes de datos.

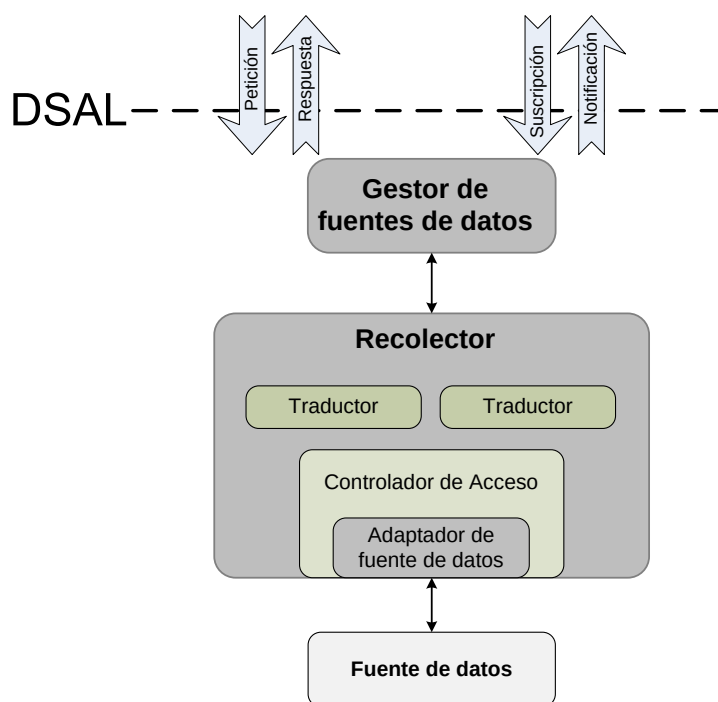


Figura 3.38: Arquitectura de la DSAL

Durante el proceso de configuración, la DSAL registra todas las fuentes de información contextual a las que local y directamente tiene acceso. En tiempo de ejecución se podrán añadir nuevas fuentes o desvincular alguna ya existente. Soporta por tanto dinamismo y escalabilidad en la integración.

La información recogida de las fuentes de contexto nativas tiene una representación propietaria. En este sentido, se asocia un recolector (*retriever*) dentro de la DSAL a cada fuente de contexto, que hace de intermediario entre el entorno propietario y la PN. Dado que conoce la idiosincrasia de la fuente de contexto a la que está vinculado, el recolector lleva a cabo las tareas de adaptación del formato de los datos recogidos al modelo de representación basado en ontologías empleado dentro de la SCMF e introducido en el apartado 3.7.4 [135]. El recolector está compuesto por un controlador de acceso, que es el encargado de la comunicación directa con la fuente de datos y al menos un traductor (*mapper*) que realiza la conversión de los datos nativos de la fuente a la representación común dentro de la SCMF. Por ejemplo, para un sensor de temperatura el controlador recoge los datos de la fuente como un voltaje, cuyo valor es proporcional a la temperatura. El ensamblador convierte ese voltaje a la métrica de medida, es decir, la temperatura en grados Celsius (°C).

El tráfico de información desde los recolectores se concentra en el gestor de fuentes de datos (DSAM, *Data Source Abstraction Manager*), entidad central en la estructura de la DSAL. Es el componente que sirve al CAM como interfaz de acceso a la información y

maneja los vínculos entre los atributos de contexto y las fuentes de contexto correspondiente. En colaboración con los recolectores y según los requerimientos impuestos por el CAM, el DSAM se encarga de lanzar los eventos ante las variaciones de los valores de los atributos.

Hasta ahora se ha mostrado principalmente a la SCMF como la fuente de contexto, pero es en la DSAL donde despliega sus capacidades de recopilación de información. La DSAL no se puede asociar a ningún nivel en particular en OSI. Se expande por todas las capas, como se describe en la figura 3.39, dado que todas contienen información contextual relevante para adaptar el comportamiento de la PN. No sólo se debe pensar en contexto como la información extraída de sensores externos, etc., sino que sondas incluidas, por ejemplo en los servicios o en la pila de comunicaciones, también reportan información para mejorar la QoS y la QoE. La aplicación del paradigma de optimización intercapas se hace aún más patente dentro de la PN gracias al gran volumen de datos que se obtiene a través de la SCMF.

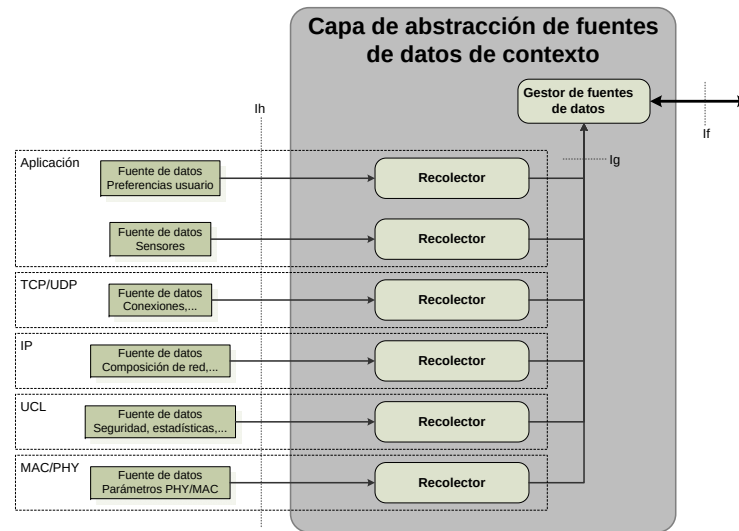


Figura 3.39: Representación de la DSAL con fuentes de datos distribuidas en los niveles OSI

3.7.1.8. Fuentes de datos

De la definición de contexto tomada [130], queda patente que el contexto es ciertamente ilimitado y por tanto el volumen de fuentes de datos puede ser tan grande como el usuario desee. En [137, 138] se muestra un conjunto de parámetros relevantes dentro de la PN, entre los que se incluyen métricas de nivel de enlace como la tasa de transmisión, la potencia empleada y la calidad del canal, el DR al que pertenece un nodo, etc.; o métricas de nivel de enlace como cantidad de errores, número de saltos medio, etc.; u otras relacionadas con la propia PN como son la composición de los *clusters*, localización de éstos, etc.

Las propias fuentes de datos únicamente ofrecen valores para los atributos que ellas pueden medir, siendo las tareas de adaptación, como ya se ha descrito, realizadas por la DSAL. De esta forma, se desvinculan los procesos de recogida de datos y el tratamiento

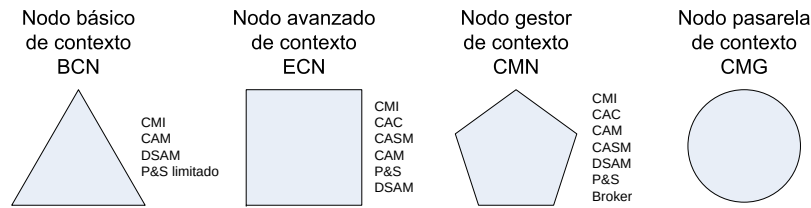


Figura 3.40: Entidades funcionales de la SCMF

de estos, pudiendo escalar el proceso de sensado tanto como se desee sin afectar a las estructuras existentes.

3.7.2. Entidades funcionales

El abanico de nodos que pueden desplegarse en una PN es muy amplio, lo que supone que no todos podrán soportar las mismas funcionalidades. Las tareas básicas asignadas a cada componente de la SCMF se resumen en:

- CMI: permitir a los CACo interrogar sobre atributos de contexto.
- CAC y NetCoM: habilitar la configuración e intercambio de información con otros nodos.
- P&S: realizar el almacenamiento y procesamiento inteligente de la información contextual tanto local como remota (bróker).
- CAM: gestionar el flujo de información y comandos dentro del agente de contexto.
- DSAL: permitir recoger información de fuentes heterogéneas de contexto.
- CASM: garantizar el acceso seguro a la información de contexto.

Teniendo esto en cuenta y agrupando capacidades según su relevancia y los requerimientos que demanden para su ejecución, se pueden definir dos entidades funcionales o tipos de nodos, tal y como se representa en la figura 3.40:

- El nodo básico de contexto (BCN, *Basic Context Node*) incluye los módulos CMI, CAM, DSAM y P&S restringidos en funcionalidades. Se trata de nodos considerados autónomos desde el punto de vista de acceso al contexto. Sin embargo, dadas las limitaciones en términos de potencia de cómputo no serán capaces de inferir información de contexto procesada y delegarán esa funcionalidad en otros.
- El nodo avanzado de contexto (ECN, *Enhanced Context Node*) dispone de mayores capacidades y por tanto está cualificado para poder procesar la información de contexto y gestionar solicitudes que requieran trabajar con múltiples fuentes simultáneamente.

Ambas entidades implementan los módulos CASM y NetCoM de manera que en todos los casos se garantiza la seguridad y la comunicación en el entorno de contexto.

Además de estas dos entidades, se pueden definir otras dos como roles especiales que tomen usualmente los ECN:

- El CMN es un ECN con la responsabilidad añadida de indexar la información contextual disponible en el *cluster*. Actúa también como intermediador de contexto para otros nodos dentro de su *cluster*, redirigiendo las consultas en caso que éstas no puedan ser respondidas en el *cluster* local. Por definición, sólo puede haber un CMN por *cluster*.
- El *Context Management Gateway* (CMG) es un nodo dedicado a establecer la comunicación con fuentes de contexto fuera de la PN.

3.7.3. Operativa general

La arquitectura de la PN lleva a distribuir las funcionalidades de forma jerárquica entre los nodos más adecuados de la PN. Cabe destacar en cierta manera las similitudes existentes con la arquitectura de red planteada para la SMP, siguiendo un enfoque centralizado dentro del *cluster* y distribuido en la PN. Esto supondrá que en muchas ocasiones los mismos nodos tomen tanto la responsabilidad desde el punto de vista de servicio como de contexto. Sin embargo, es importante resaltar que si bien en el caso de la SMP existen múltiples protocolos y mecanismos para la administración de servicios, en el caso de la SCMF éstos se han desarrollado ajustándose a la PN [136, 139].

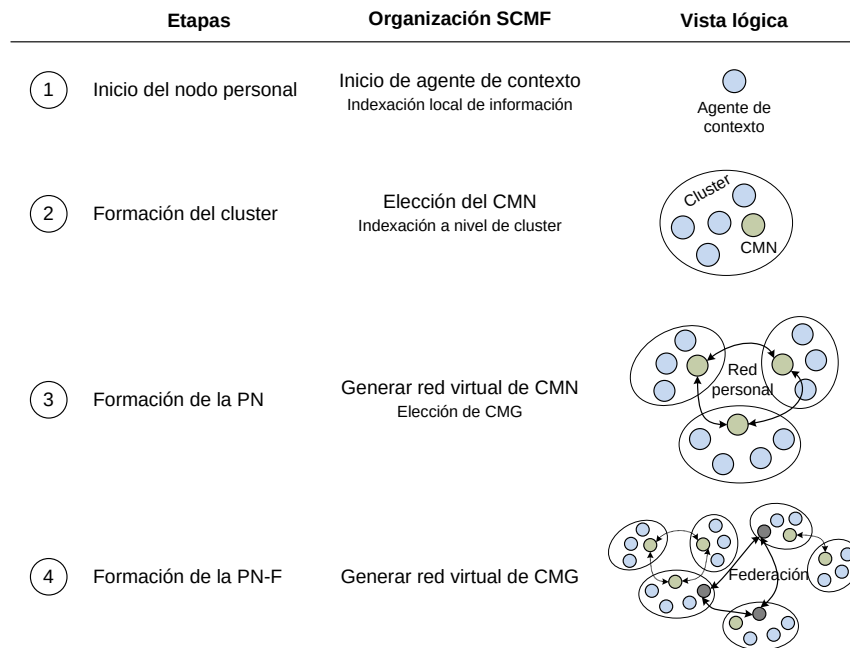


Figura 3.41: Etapas en la operativa de la SCMF

La figura 3.41 presenta el proceso de establecimiento y organización de la SCMF sustentado en los agentes de contexto residentes en cada nodo. Al iniciarse un agente de contexto éste lee, actualiza e indexa la información disponible localmente. El siguiente paso consiste

en descubrir la identidad del CMN dentro de su *cluster*. Así, dado que el rol de CMN lo ostenta aquel agente de contexto con mayores capacidades, el nodo que se acaba de iniciar lanza un mensaje de reto con sus capacidades, lo que permite, mediante un procedimiento de contienda, determinar quién es el nodo más adecuado. Para reducir la complejidad del proceso, se introducen las capacidades potenciales de gestión de contexto a una función de coste que de manera genérica devuelve un valor, denominado peso asignado al nodo de contexto (CNW, *Context Node Weight*), que resume las funcionalidades disponibles. Como resultado de la contienda un nodo ECN se erige como CMN. El CMN periódicamente publica su identidad y capacidades asociadas de forma que, en caso de que algún nodo sea más potente, pueda solicitar un traspaso de papeles y así atender mejor a las necesidades asociadas al contexto dentro de la PN [123]. En el capítulo 6 se ofrece la descripción, implementación y validación de una solución para llevar a cabo el procedimiento anterior.

Por defecto las peticiones se procesan y resuelven localmente siempre que sea posible. La interacción entre los CACo y la SCMF se realiza a través del CMI de su agente de contexto y por tanto siempre a nivel local. Aunque sea necesario lanzar las peticiones a nodos remotos, este comportamiento queda oculto para los CACo.

Para resolver una solicitud de contexto, primeramente se ha tenido que realizar el registro del recolector de una fuente de datos compatible. La solicitud incluirá, además del atributo, el tipo de acción a tomar (suscripción, respuesta puntual, etc.). También se podrán adjuntar criterios como el rango temporal o espacial de búsqueda.

Tanto las peticiones como las suscripciones deben ser autorizadas por el CASM. Internamente, una vez aceptadas, ambas se gestionan de una forma similar, asignando un identificador único que vincula dentro del CAM los atributos, la acción y el CACo generador de la consulta. En el caso de las suscripciones, el CAM debe decidir en función del modo incluido (periódico, valor de referencia, etc.) si generar o no una notificación hacia el CACo. Hay que reseñar que los CACo no tienen por qué ser siempre entidades externas. En la propia operativa del agente de contexto, existen módulos como el P&S o el CASM que requieren acceso a información contextual. Para uniformizar la operativa, estos módulos podrán ser considerados como CACo.

Las peticiones que se resuelven a nivel local se remiten por valor. Sin embargo, cuando la petición tiene que ser redirigida al CMN, éste puede proporcionar la respuesta asociada bien por valor o por referencia, dependiendo de las preferencias impuestas. En todo caso, como se ha dicho, es preferible que se retorne únicamente el valor para el caso de nodos demandantes poco potentes. Esta operativa redundante además en la ocultación de la fuente de los datos. El formato de la respuesta también está estrechamente ligado al nivel de seguridad que se haya planteado en la PN.

En la figura 3.42 se muestra un ejemplo de las interacciones dentro del *cluster*. En todos los casos los extremos de los intercambios son los CAM de cada nodo.

Una vez se hayan agotado las posibilidades de encontrar la información en el *cluster*, la búsqueda se extiende a toda la PN. Tal como se puede observar en la figura 3.43, los CMN serán los encargados de redirigir las solicitudes pendientes. No obstante, dado que las peticiones de contexto pueden llegar a ser muy elevadas en número y puesto que tanto los ECN como los BCN incluyen un módulo de comunicaciones, con el objeto de reducir las res-

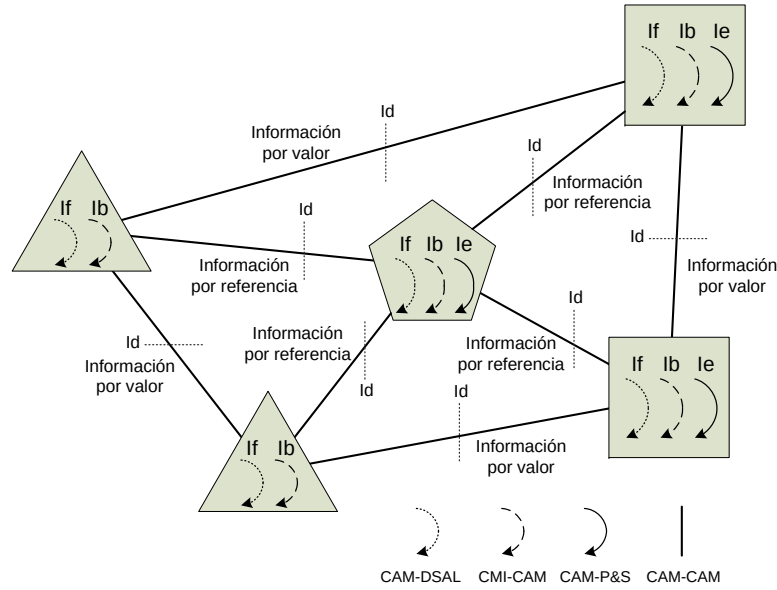


Figura 3.42: Interacciones en la SCMF a nivel de *cluster*

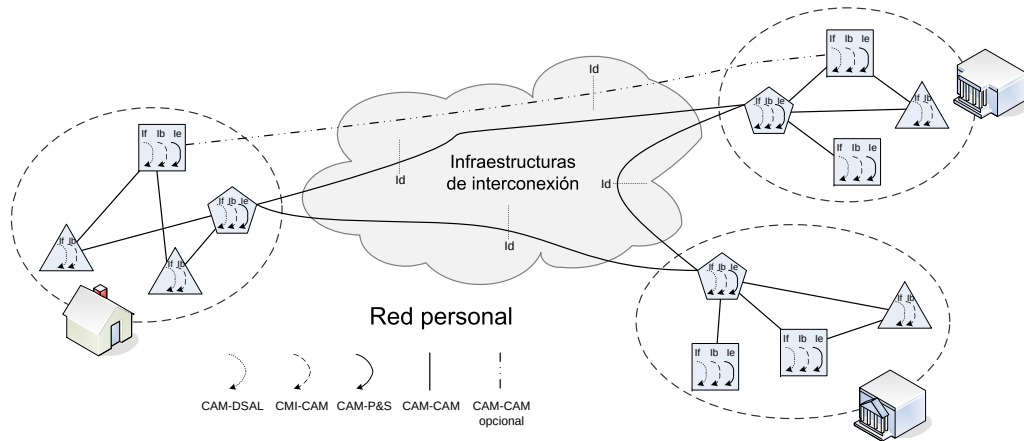


Figura 3.43: Interacciones en la SCMF a nivel de PN

ponsabilidades del CMN se permite a los ECN y los BCN de *clusters* distintos comunicarse directamente.

3.7.4. Modelado del contexto

En las secciones anteriores se ha hecho mención a dos módulos a través de los cuales es accesible la información de contexto. Por un lado, la DSAL aporta el origen del contexto, mientras que a través de la capa de acceso al contexto las aplicaciones, servicios o cualquier otro elemento recogen el contexto, abstrayéndose de los procesos que lleva su gestión dentro de la SCMF.

Tan importante como las metodologías de recolección o procesado es la forma en la que la información se representa. Se pueden distinguir dos formatos de información:

- Datos nativos no procesados recogidos directamente de las fuentes (sensores, etc.)
- Información de contexto procesada que se ajusta a un modelo y formato de representación de datos.

Los datos nativos se representan en formatos propietarios y es gracias a un modelo unificado que esa información se convierte en contexto, permitiendo su compartición y gestión por diferentes entidades. En el caso de la SCMF el modelo de representación del contexto debe ser lo más genérico posible, incluyendo cualquier objeto o atributo asociado directamente al usuario, pero también a su entorno.

La definición semántica del contexto debe proporcionar un acceso eficiente y facilitar la inclusión de nuevos objetos de manera sencilla sin tener que modificar ni el lenguaje de descripción ni los interfaces. Existen multitud de opciones para modelar la información de contexto [140] si bien no todas se ajustan al escenario de la PN. Por ejemplo, modelos basados en etiquetas o duplas llave-valor son simples en su representación pero de difícil uso cuando describen sistemas moderadamente complejos.

Para el caso de la PN se pueden destacar modelos orientados a objetos, modelos basados en ontologías o el *Presence Information Data Format* (PDIF) [141], entre otros. PDIF emplea el concepto de entidades definidas a partir de la información de presencia, lo que supone por ejemplo que una persona se modelaría a través del uso de los servicios en sus dispositivos. Por su parte, los modelos orientados a objetos representan las entidades como un conjunto de atributos heredables de padres a hijos. Si bien estos dos modelos podrían servir como base para describir la PN, se observan ciertas restricciones que hacen que no puedan cumplir todas las necesidades de la PN.

Los modelos basados en ontologías extienden de alguna manera los orientados a objetos. Realizan una descripción formal de los conceptos y sus propiedades bastante similar, pero adicionalmente permiten modelar las relaciones entre las instancias de los objetos. Todo ello hace viable un aspecto muy interesante desde el punto de vista de contexto, el razonamiento. Las ontologías se pueden considerar como un vocabulario común con unas reglas básicas fijadas que vinculan los conceptos, a partir de las cuales empleando los motores cognitivos adecuados se pueden inferir relaciones no directas y más complejas.

Por tanto, el uso de ontologías dentro de la PN se intuye como el modelo más adecuado. OWL [142, 143] se considera el estándar *de facto*. Se trata de una familia de lenguajes para generar ontologías basado en tripletas (sujeto-verbo-predicado), que van desde el más genérico y global, OWL Full, hasta las versiones ligeras, OWL DL y Lite. A mayor complejidad más recursos computacionales se requieren para procesar las tripletas e inferir nuevas relaciones. Con el fin de conseguir llegar al mayor número de nodos dentro de la PN, incluidos aquellos menos potentes, se recomienda usar las restricciones impuestas por el modelo OWL DL o Lite (p. ej. la forma de definir clases, las condiciones de transitividad, etc.).

En la figura 3.44 se presenta un extracto de la representación básica para una PN, donde se ejemplifica la descripción del nodo personal. La forma de generar la ontología se basa en el paradigma de orientación a objetos, siendo los atributos del padre heredados por los hijos, permitiendo restricciones en casos particulares. Por ejemplo, un nodo es todo dispositivo

que tiene una dirección IP, por lo que el atributo o propiedad `implementsIP` debe ser afirmativa en cualquier nodo.

Por otro lado, todo nodo de la PN debe estar asociado a un usuario e incluir un identificador. Es por esto que la ontología define atributos como `hasIdentifier`, `isPersonal` o `hasTrustRelationship`. Además impone un axioma o regla de relación de atributos por la cual si un nodo no tiene el atributo `isPersonal` no podrá establecer una relación `hasTrustRelationship` con ningún otro.

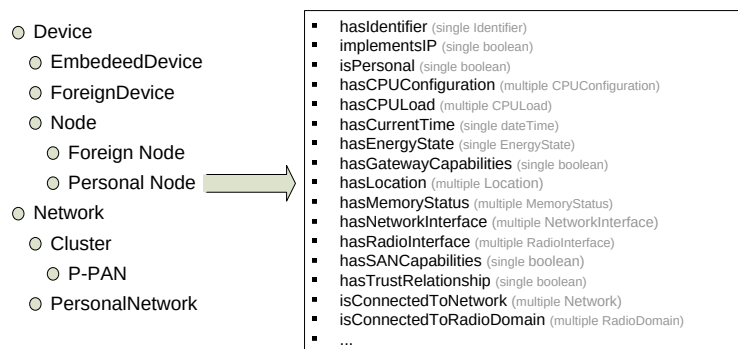


Figura 3.44: Descripción de la entidad Nodo Personal (`Personal Node`)

Pero además de representar las entidades de la PN, la ontología debe servir para describir de la forma más adecuada el contexto. Por tanto, a la descripción básica se le añade meta-información, tal como el momento de la última actualización, validez temporal, etc. Estos metadatos darán consistencia a los datos para poder ser considerados como información contextual.

3.7.5. Lenguaje CALA

Los CACo y la SCMF interactúan a través del CMI empleando el lenguaje CALA. CALA define los métodos necesarios para habilitar el acceso a la información contextual de forma síncrona y asíncrona, así como para modificar la información.

El lenguaje CALA se estructura en cuatro grandes campos:

- Entidades y sus atributos: referencia la información de contexto a la que se quiere acceder. Las peticiones o suscripciones pueden hacerse basándose en identificadores conocidos o bien en base a un tipo. Junto a la entidad se recomienda incorporar la lista de atributos a recoger.
- Restricciones: limita, mediante operaciones lógicas, los valores de uno o más atributos que se retornen.
- Alcance o dimensión: determina el dominio de búsqueda sobre el que realizar la búsqueda. Su valor puede vincularse desde el punto de vista de PN (nodo, *cluster*, PN, etc.), o venir dado por localización física absoluta, por unidades temporales, etc.

- Opciones: incluye información adicional y extensiones a la información básica. Dentro de ella se encuadran todos los aspectos relacionados con la seguridad en el acceso al contexto (credenciales, etc.)

Además de estos campos genéricos, las operaciones asíncronas requieren de un campo específico que caracteriza las condiciones bajo las cuales las actualizaciones del contexto se deben notificar al peticionario. Entre el conjunto de cláusulas se incluyen:

- Notificar una única vez cuando recoger la respuesta a una determinada petición puede demorarse durante mucho tiempo, registrando un evento de forma que el CACo no esté bloqueado durante ese tiempo. Es el caso de, por ejemplo, determinar los nodos vecinos con WLAN activada, donde el proceso de escaneo dura varios segundos.
- Notificar al superar un nivel de referencia, implementando un proceso de histéresis para evitar eventos continuos en los límites; con esta configuración se permite lanzar un evento ante un cambio en un valor numérico, referenciado de forma absoluta o relativa.
- Notificar de forma periódica.

Para seguir el estado de las suscripciones, a cada petición se le asigna un identificador único asociado al CACo.

A continuación se incluyen una serie de ejemplos que permiten comprender mejor la operativa y la sintaxis de CALA. La figura 3.45 muestra una solicitud de información sobre la que se interroga a la SCMF por la localización de la entidad Bob en la localización Edificio X. La respuesta asociada presenta dos posibles localizaciones, cada una de ellas con un grado de confianza, incluido en forma de metadato. A la vista de los resultados obtenidos lo más probable es que Bob se encuentre en Sala 2 dentro del Edificio X.

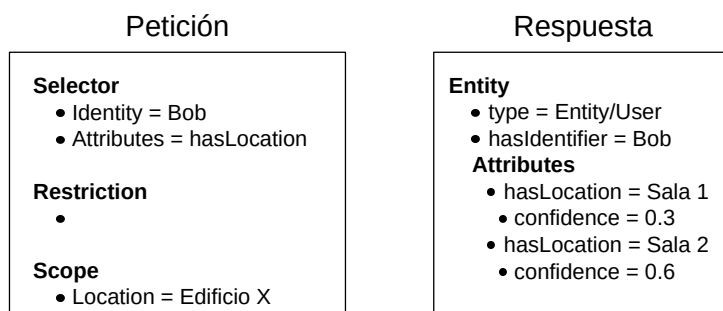


Figura 3.45: Ejemplo de petición-respuesta en lenguaje CALA

El extracto de código del cuadro de texto 3.1 muestra un ejemplo de un documento XML que incluye una petición realizada en lenguaje CALA, en la que se interroga por características de un elemento de la PN asociada al usuario con nombre John Doe.

El lenguaje CALA soporta la actualización de información de contexto. Las peticiones llevarán en este caso asociado el valor que debe tomar el atributo que se desee modificar. De

Cuadro de texto 3.1: Ejemplo de codificación de una petición en lenguaje CALA

```
<query>
  <selector>
    <hasIdentifier>[unique identifier]</hasIdentifier>
    <attributeName>
      http://www.ist-magnet.org/2006/08/02/MagnetContextOntology.owl/hasName
    </attributeName>
    <attributeName>
      http://www.ist-magnet.org/2006/08/02/MagnetContextOntology.owl/hasPN
    </attributeName>
  </selector>
  <restriction>
    <operator>AND</operator>
    <operand>
      <operator>EQUALS</operator>
      <operand>
        <attributeName>
          http://www.ist-magnet.org/2006/08/02/MagnetContextOntology.owl/hasName.
          firstName
        </attributeName>
      </operand>
      <operand>
        <value>John</value>
      </operand>
    </operand>
    <operand>
      <operator>EQUALS</operator>
      <operand>
        <attributeName>
          http://www.ist-magnet.org/2006/08/02/MagnetContextOntology.owl/hasName.
          lastName
        </attributeName>
      </operand>
      <operand>
        <value>Doe</value>
      </operand>
    </operand>
  </restriction>
  <scope>
    <domain>PN</domain>
    <location/>
    <time/>
  </scope>
  <options/>
</query>
```

esta forma, los servicios o cualquier otra entidad, incluido el propio usuario, podrán modificar directamente información de contexto. Es importante señalar que estas modificaciones no son libres, sino que siempre vendrán garantizadas al tener que atravesar el CASM.

Capítulo 4

Seguridad y privacidad

La PN refleja la visión de una red centrada en el usuario, en la que éste potencialmente dispone de una plétora de dispositivos, con diferentes capacidades y tecnologías de comunicación heterogéneas. Los nodos dentro de una PN se agrupan en *clusters* definidos por la relación de confianza existente entre sus miembros. Los nodos pertenecientes a un mismo *cluster*, y que generalmente son cercanos entre sí, pueden comunicarse entre ellos sin necesidad de apoyarse en otros nodos cuya identidad no haya sido confirmada. Hasta el momento se han definido los procedimientos para hacer de la combinación de nodos personales una PN e incluso eventualmente permitir la comunicación con nodos externos. Todo ello se ha orientado a hacer de la PN una red auto-configurable que se gestione de la forma más transparente posible a la vez que ofrezca un valor añadido al usuario.

Dicho esto, uno de los principales objetivos de la PN es lograr que la red del usuario sea una red segura. La seguridad no sólo se centra en proporcionar un establecimiento y uso seguro de la PN, garantizando la privacidad de las comunicaciones entre los dispositivos y nodos de usuario, sino también la transparencia en su despliegue. Las medidas de seguridad que implemente una PN deben exportarse más allá del nivel de red, haciendo que los servicios propios o de otros usuarios o proveedores de confianza sean accesibles con garantías dentro de la PN.

La seguridad dentro de una PN se basa en el fuerte vínculo existente entre los nodos personales, hecho que se hace patente con el establecimiento de una relación bilateral de confianza fijada por el usuario. Se pueden distinguir dos tipos de protección cuando dos nodos personales se comunican: seguridad extremo a extremo o en cada salto. Si bien la primera opción es la más recomendable, supone que los dos extremos de la comunicación son de confianza, condición que no siempre se da. En la otra situación, la PN garantiza que los saltos intermedios necesarios que involucren nodos personales son seguros y confiables. En cualquiera de los casos, las comunicaciones dentro de la PN son seguras por naturaleza, independientemente de la aplicación o servicio que se ejecute y la tecnología de comunicaciones que se emplee. Esto se consigue apoyándose en mecanismos de seguridad estándar o en soluciones propietarias de la PN superpuestas a las anteriores en caso de detectar deficiencias en las tecnologías.

El esfuerzo en la definición y despliegue de una plataforma de seguridad para la PN no se tiene que concentrar en resolver problemas puntuales y específicos, sino que tiene

que aspirar a ser una solución integral que englobe las necesidades de seguridad en todos los niveles, considerando al usuario, sus servicios, la heterogeneidad de sus dispositivos, etc. A continuación se definen las bases para la gestión de la seguridad dentro de la PN, desarrollando el protocolo que permite implantar la relación de confianza entre los nodos. Esta relación de confianza evolucionará hacia un concepto más genérico que soporte la diversidad de la PN en todas las capas de abstracción definidas.

4.1. Terminología

Establecer una terminología y acordar las definiciones de los conceptos facilita el seguimiento de las consideraciones posteriores. Es por esto que en la tabla 4.1 se describen los conceptos más importantes relacionados con la seguridad en la PN.

Tabla 4.1: Terminología de seguridad

Términos comunes	
Clave (<i>Key</i>)	Secuencia de bits única con la que controlar el comportamiento de los algoritmos criptográficos empleados para cifrar información.
Relación de confianza (<i>Trust Relationship</i>)	Condición existente entre entidades que determina el grado de certidumbre en la validez de sus credenciales, habilitando la autenticación mutua y el establecimiento de un canal seguro de comunicaciones entre ellos.
Marcado (<i>Imprinting</i>)	Procedimiento seguro mediante el cual se establece la relación de confianza entre dos nodos.
Canal autenticado en proximidad (<i>Proximity Authenticated Channel</i>)	Canal de comunicaciones entre dos dispositivos o nodos autenticado por el usuario empleando medios físicos, lo que implica la interacción directa del usuario sobre ambos nodos.
Transitividad	Propiedad dentro de la PN por la que la relación de confianza de dos entidades con un intermediario autoriza el establecimiento de la relación directa entre esas dos entidades. Esta propiedad permite extender de forma automática y transparente los vínculos entre nodos personales.

4.2. Notación

En la descripción de los protocolos empleados para proporcionar la seguridad dentro de la PN se emplea la notación incluida en tabla 4.2.

Tabla 4.2: Nomenclatura empleada en seguridad

Símbolo	Significado
ID_X	Identidad de X
$E_K(m)$ o $E(K, m)$	Cifrado simétrico de los datos m empleando la clave K
$h(m)$	Función hash de m
$h_K(m)$	Función hash de m con clave K
N_X	Número aleatorio o <i>nonce</i> generado por X
PK_X	Clave pública de X
SK_X	Clave privada de X
$S_X(m)$	Firma de los datos m usando la clave privada de X
$P_X(m)$	Cifrado de datos m empleando la clave pública de X
$Cert_X$	Certificado que vincula la identidad de X con su clave pública
$\parallel$	Concatenación

4.3. Procedimiento de marcado

La arquitectura de seguridad dentro de una PN se basa en la relación bilateral de confianza entre los nodos y dispositivos personales. Los nodos personales se emparejan de forma segura, lo que habilita el reconocimiento y la comunicación segura entre ellos. Cuando un nuevo nodo se empareja por primera vez con uno personal ya existente, se considera que el nuevo nodo está marcado y pasa a ser un nodo personal. El hecho de marcar un nodo supone que ese dispositivo establece una relación de confianza a largo plazo con al menos otro dispositivo dentro de la misma PN.

El sellado de nodos se basa en el protocolo de formación de la PN (PFP, *PN Formation Protocol*), cuya satisfactoria finalización supone que el nuevo nodo pasa a formar parte de la PN. Resultado de la ejecución de este proceso, los nodos comparten unas claves criptográficas bilaterales que sostienen la relación de confianza a largo plazo. Dada la importancia de estas claves de las que depende la estructura de la PN, su generación debe realizarse en unas condiciones especiales que garanticen la estanqueidad del proceso evitando poner en riesgo a la PN:

- El usuario tendrá el control total sobre la forma de ejecutar el procedimiento de marcado, es decir, determinará cuándo y cómo el nuevo dispositivo se marcará y pasará a formar parte de su PN. Posteriormente, a nivel de conectividad y de red, todos los dispositivos o nodos personales son igualmente confiables. A nivel de servicio, aunque la seguridad en principio está también asegurada, quizás haya que aplicar condiciones adicionales para confirmar el proveedor y consumidor final.

- Los potenciales nodos o dispositivos personales comparten dos interfaces de comunicación diferentes:
 - Canal autenticado en proximidad (PAC, *Proximity Authenticated Channel*) por el usuario empleando medios físicos.
 - Canal de comunicación cableado o inalámbrico sobre el que se realiza el intercambio de datos entre los dispositivos encapsulados usando un protocolo de nivel de red o de conectividad.

El primer emparejamiento de un nodo con otro personal se produce empleando un PAC y asistido por el usuario. Este tipo de canal requiere que el usuario se encuentre en las proximidades del dispositivo, pudiendo identificarlo e interactuar con él. El PAC o parte de él se puede establecer sin que exista una conexión entre los nodos. Normalmente la metodología de autenticación por proximidad que se define sobre el PAC se basa en tocar el dispositivo, pulsar algún botón o bien la lectura y posterior introducción de un código a través de los interfaces de acceso (teclado, pantalla, cámara, etc.). En aquellos dispositivos que carezcan de estas interfaces, el PAC se podrá habilitar almacenando la información a intercambiar (su identidad, etc.) en medios externos como tarjetas identificación por radio frecuencia (RFID, *Radio Frequency IDentification*), códigos de barras o QR durante el proceso de fabricación.

Según el nivel de seguridad que el PAC proporciona se pueden distinguir dos tipos: un PAC privado que garantiza la autenticidad, integridad y confidencialidad y otro público que sólo provee autenticidad e integridad. Debido al riesgo que conlleva la posible captura de la información intercambiada a través de un PAC público, se requiere que la información que se transmite no esté correlada y su longitud sea al menos de 160 bits para evitar una fácil manipulación. En caso de detectar un riesgo manifiesto incluso en esas circunstancias se recomienda emplear un PAC privado siempre que sea posible [107]. Un ejemplo de PAC privado consiste en la lectura, por parte de un usuario, de una cadena de caracteres alfanuméricos de la pantalla de un dispositivo, únicamente visibles para él, e introducirlos mediante el teclado en el otro dispositivo. Claramente este canal supone ciertas limitaciones de uso, pues para ser amigable la cadena de caracteres no debe ser extensa. No obstante, es un reflejo de la sencillez de un PAC privado, como podría ser también el pulsar un botón o el propio dispositivo. Por su parte, un ejemplo de PAC público puede realizarse empleando etiquetas basadas en RFID, comunicaciones infrarrojas o códigos de barras o QR, donde, durante el proceso de fabricación, se almacenaría la información a intercambiar a posteriori. Esta solución es adecuada cuando el dispositivo carece de interfaces de interacción con el usuario.

No obstante, la reciente proliferación de tarjetas inteligentes y la irrupción de los dispositivos con interfaz de comunicaciones de campo cercano (NFC, *Near Field Communication*) añaden un nivel más en términos de confianza y confidencialidad a los sistemas basados en RFID como elementos para implementar un PAC. En este sentido, las tarjetas inteligentes y los dispositivos que implementan NFC tienen las capacidades de cómputo suficientes como para salvaguardar la identidad y generar los parámetros necesarios para llevar a cabo el procedimiento de marcado. Estos dispositivos incluyen un *hardware* diseñado para soportar eficientemente operaciones criptográficas y la disminución considerable de su coste de fabri-

cación hace que cada día estén más presentes en los terminales de usuario de uso cotidiano (teléfonos móviles, tabletas, portátiles, etc.). Hacer que el usuario pueda personalizar sus nodos de una forma sencilla sólo con acercarlos, siguiendo el paradigma *touch and go*, y empleando en la mayoría de los casos el mismo procedimiento, no es sino un avance en lo que a la generación de una PN se refiere [144-146].

4.3.1. Descripción del protocolo

El PFP se diseña considerando que el establecimiento de la confianza entre los nodos se realiza en dos etapas:

1. Intercambio de información para una primera autenticación vía PAC. La elección del tipo de PAC depende del dispositivo y las interfaces de usuario.
2. Ejecución del protocolo de generación de claves bilaterales compartidas sobre un canal de comunicación inseguro, autenticado basándose en la información intercambiada en el paso anterior.

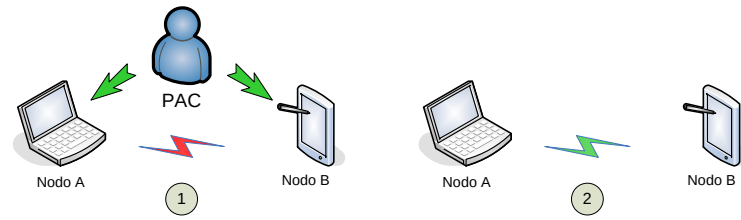


Figura 4.1: Escenario de ejecución del protocolo de marcado

Ambas etapas se tienen que completar para personalizar un nodo y hacerlo accesible dentro de la PN. El protocolo soporta la ejecución no consecutiva de éstas, aunque es obligatorio que la primera parte se ejecute con antelación a la segunda. La figura 4.1 incluye el escenario de ejecución del proceso.

Definido en el ámbito del proyecto MAGNET, el protocolo de marcado se basa en algoritmos de clave asimétrica, típicamente en el protocolo *Diffie-Hellman* (DH). Se recomienda emplear grupos DH dentro de los estandarizados sobre criptografía basada en curvas elípticas (ECC, *Elliptic Curve Cryptography*) de tamaño suficiente [147]. Estos grupos han sido estandarizados desde el National Institute of Standards and Technology (NIST), el IETF y más recientemente por el ETSI para la European Electronic Signature Standardisation Initiative (EESSI).

En la figura 4.2 se describe el protocolo y la secuencia de mensajes que se intercambian los nodos. La descripción del protocolo es independiente del grupo DH seleccionado y emplea notación genérica donde g es el elemento generador:

1. Parte 1: Intercambio sobre PAC
 - 1a) B genera su secreto DH, b , y calcula su clave pública $K_B = g^b$. También genera el hash de K_B y lo envía junto con su identidad ID_B a A .

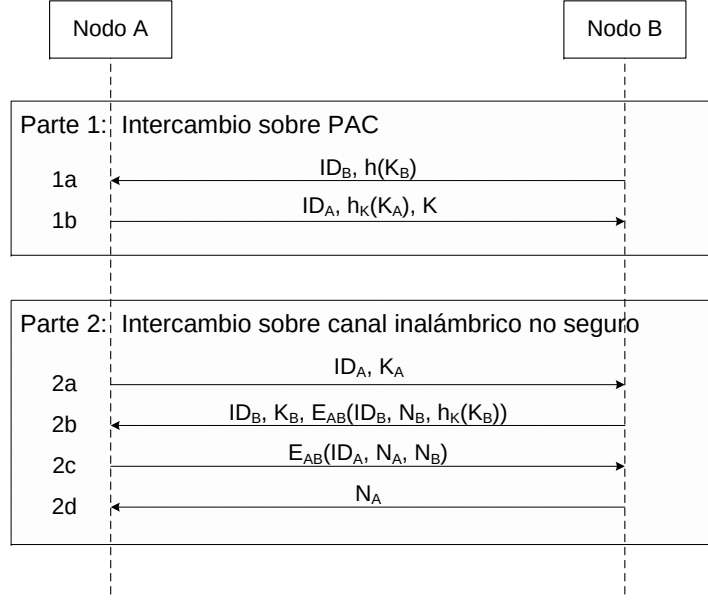


Figura 4.2: Protocolo de marcado

- 1b) A genera su secreto DH, a , y calcula su clave pública $K_A = g^a$. También genera una clave K y computa el hash de K_A usando K . Finalmente envía el hash, la clave K junto con su identidad ID_A a B .
2. Parte 2: Intercambio sobre canal inalámbrico no seguro
 - 2a) A envía su identidad ID_A y la clave K_A a B .
 - 2b) B verifica K_A a partir de K y $h_K(K_A)$. Calcula la clave K_{AB} compartida entre A y B como el hash $h(g^{ab})$. Autentica su clave K_B empleando $h_K(K_B)$ y genera un número aleatorio N_B . Cifra todo junto con su identidad ID_B empleando la nueva clave K_{AB} y remite el resultado junto con ID_B y K_B a A .
 - 2c) A recibe K_B y calcula la clave compartida K_{AB} como el hash $h(g^{ab})$. Extrae del mensaje recibido N_B y $h_K(K_B)$ y verifica K_B basándose en $h_K(K_B)$. Tras esto A genera un número aleatorio N_A y lo cifra y autentica junto a N_B usando la clave K_{AB} . El resultado lo transmite a B .
 - 2d) B descifra el mensaje usando K_{AB} , extrae N_A y se lo transmite a A .

Tanto A como B calculan la clave bilateral compartida o clave personal entre ellos, $K_{PN}(A, B)$, empleando la función de resumen cifrado HMAC-SHA-256^{1,2}, tal que $K_{PN}(A, B) = h_{K_{AB}}(N_A || N_B)$

Aunque existen diferentes combinaciones dependiendo del PAC que se emplee, se recomienda que el procedimiento se implemente de forma completa para garantizar el correcto

¹ *keyed-Hash Message Authentication Code* (HMAC)

² *Secure Hash Algorithm* (SHA)

marcado en cualquier situación. Si el PAC empleado es privado, el mensaje 1a puede omitirse y emplear una clave K más corta sin menoscabo de la seguridad. Esta operativa favorece el uso en PAC privados que normalmente ofrecen un pequeño ancho de banda. Por el contrario, si el PAC es público el secreto K quedaría comprometido y no tiene sentido transmitirlo, por lo que se considera $K = \emptyset$. En este caso se recomienda emplear funciones de hash que generen códigos más largos con al menos 160 bits. Para ambos PAC los mensajes 2b y 2c permiten vincular de forma fiable las identidades de los nodos con las claves que intercambian.

La identidad de cada nodo debe ser única en la PN. En el apartado 3.5 se asoció la dirección personal a nivel de red de cada nodo al identificador del nodo dentro de la PN. Este identificador tiene que estar vinculado al nodo en cuestión durante toda su vida útil. En este sentido, los 48 bits de las direcciones MAC de las interfaces de red son únicas, por lo que se presentan como un buen candidato para definir el identificador personal. En caso que el nodo disponga de varias interfaces, la UCL oculta todas sobre una virtual, generada a partir de las existentes, que sería la idónea para ser usada. Dado que la dirección MAC es pública, el usuario puede desear no emplearla directamente como identificador personal. En ese caso la identidad podría diversificarse a partir de esa dirección usando un valor o identificador generado por el usuario (UGI, *User Generated Identifier*), resultando por ejemplo:

$$ID_X = h(UGI_X \parallel \text{dirección MAC}(X))$$

Al finalizar el procedimiento, los dispositivos o nodos A y B comparten una clave bilateral $K_{PN}(A, B)$ en la que se basa la relación de confianza mutua a largo plazo y a partir de la cual se securizan todas las comunicaciones entre ese par de nodos. Se trata de una clave para operar sobre algoritmos de criptografía simétrica. Estos algoritmos se caracterizan por su menor latencia y una integración más sencilla en plataformas *hardware*. Estas características dan soporte a las necesidades de seguridad de las comunicaciones dentro de la PN.

La ejecución del PFP se realiza a nivel de enlace empleando tecnologías de comunicaciones compartidas por ambos dispositivos. Se ha optado por esta operativa para permitir que todos aquellos dispositivos que no implementen soporte de nivel de red (p. ej. IPv4 o IPv6) puedan llevar a cabo el proceso de emparejamiento y pasar a formar parte de la PN. Adicionalmente, puesto que el protocolo se basa en un intercambio directo entre dos entidades, el nivel de enlace parece el más natural de usar, ya que obliga a tener los nodos dentro del rango de cobertura a distancia uno, sin tener que apoyarse en nodos externos. Si a esto se le une la supervisión del proceso por parte del usuario, hace que tanto sobre el PAC como sobre el canal inalámbrico no seguro sea más compleja la existencia de ataques, especialmente de hombre en el medio (*man-in-the-middle*) [148, 149].

Considerando la operativa de la PN, parece lógico pensar que, aunque el proceso de marcado esté guiado por el usuario, las entidades o componentes PN residentes en los nodos puedan servir de apoyo en el proceso, especialmente de descubrimiento de nodos. La UCL como gestora de las diferentes interfaces de comunicación disponibles en el terminal se erige como la entidad más adecuada para proporcionar esta ayuda. Unidas a las capacidades del módulo de descubrimiento de vecinos, está facultada para detectar nuevos nodos operando

en el mismo DR. El descubrimiento de un nuevo vecino no personal dispararía el proceso de marcado, solicitando al usuario completar las acciones necesarias sobre el PAC o si éstas ya se han realizado con anterioridad, finalizando el proceso.

4.3.2. Gestión de claves

Una vez generadas las claves compartidas bilaterales de largo plazo es responsabilidad de cada nodo, y en su defecto del usuario, el garantizar su correcto almacenamiento. Cada clave debe tener asociada al menos la siguiente información:

- Nombre del nodo: identificador asociado por el usuario al nodo.
- Identificador único del nodo: identidad personal asociada unívocamente al nodo tal como se describió anteriormente.
- Clave PN (K_{PN}): clave bilateral compartida con el nodo, generada a través del PFP.

Además de estos valores, se puede asociar esta base de datos con la generada por el módulo de descubrimiento de vecinos de la UCL, de forma que en un único lugar se disponga de toda la información relativa a las claves de seguridad, número de interfaces del nodo, dirección personal, etc.

Todos los dispositivos tienen la capacidad para almacenar al menos un registro en su base de datos. Los dispositivos con poca memoria o pocas capacidades de cómputo necesitarán repetir el procedimiento PFP más a menudo, ya que sobrescribirán registros de su base de datos en los que almacenen la información relativa a otros nodos. Para tratar de mantener el listado de nodos dentro de unos límites se puede optar por implementar un mecanismo de permanencia en función de la frecuencia de comunicación con un determinado nodo. De esta forma, se revocará la relación de confianza con aquellos nodos con los que no se haya comunicado durante un período de tiempo.

Como medida de prevención, aunque se supone que las claves bilaterales con validez a largo plazo obtenidas tras el PFP asocian a dos nodos durante toda su vida, también se puede fijar un tiempo de expiración, superado el cual se revoca la relación de confianza.

Es importante reseñar que la información de seguridad relativa a los nodos personales debe estar disponible en todas las capas de abstracción, desde la capa de abstracción a nivel de conectividad hasta los niveles de servicio y contexto. Aunque esta información esté accesible, esto no implica que se utilice directamente. Para preservar la integridad y confidencialidad de las claves maestras, en cada nivel se deben generar claves específicas derivadas de la clave K_{PN} . Dichas claves tendrán una validez temporal limitada restringida a la duración de una sesión, entendiendo sesión como un procedimiento atómico en cada respectivo nivel de abstracción.

4.3.3. Propiedad de transitividad

Establecida la relación de confianza entre al menos dos nodos empleando el PAC como canal, existe, como ya se ha introducido, la posibilidad de propagar esa confianza entre

nodos mediante intermediarios usando la propiedad de transitividad. Aunque todas las comunicaciones dentro de la PN están garantizadas salto a salto, en ciertas ocasiones puede resultar necesario establecer una comunicación segura extremo a extremo entre dos dispositivos personales.

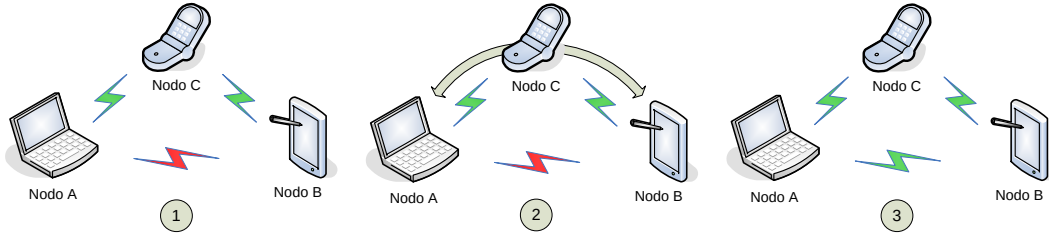


Figura 4.3: Propagación de la confianza mediante la propiedad de transitividad

Supóngase un escenario con tres nodos, como el reflejado en la figura 4.3, donde dos de ellos (A y B) han establecido una relación de confianza con el tercero (C) pero no entre ellos. En este sentido, dado un nodo que mantiene una relación de confianza con un par de nodos de forma independiente, este nodo puede interactuar con ambos para establecer la relación de confianza entre los otros dos nodos. Este proceso de emparejamiento puede realizarse de forma automática asegurando la comunicación con las claves bilaterales existentes.

Una posibilidad para establecer la relación de confianza entre A y B sería delegar en C el proceso de generación de la clave personal $K_{PN}(A, B)$ y que fuera éste quien se la remita a cada uno de los nodos. Si bien la PN se sustenta en la confianza entre los nodos personales, delegar la generación de esa confianza en un tercero, aunque asumible como riesgo de seguridad, no es la mejor opción puesto que ese nodo podrá reemplazar a cualquier de los otros dos nodos al conocer la clave compartida entre ambos.

Por tanto es necesaria una alternativa que elimine ese agujero de seguridad. La propiedad de transitividad puede ser la solución. Se basa en emplear los canales de comunicación seguros establecidos con el tercer nodo para reemplazar el uso de un PAC. De esta forma el tercer nodo no podrá reemplazar la identidad de ninguno de los otros dos pues no tendrá acceso a la clave compartida que mediante el PFP deriven.

No es obligatorio que todos los nodos o dispositivos personales tengan la capacidad de poder hacer uso de la propiedad de transitividad. Lo más común y útil es que los nodos que sirvan de puente entre dos DR incorporen esta funcionalidad, logrando de esta forma que la heterogeneidad de tecnologías de comunicación dentro de la PN no sea un impedimento para que los nodos personales se emparejen. En estas situaciones, la comunicación directa a través de un túnel seguro sirve de canal para que los nodos se asocien. En la figura 4.4 se incluye un diagrama con el procedimiento asumiendo que todos los nodos comparten la misma interfaz de comunicaciones.

4.4. Procedimiento de marcado certificado

La negociación de claves es una técnica que se aplica para que dos extremos que desean establecer una comunicación segura entre ellos generen una clave compartida que permita asegurar dicha comunicación. Normalmente la clave derivada está vinculada a algoritmos

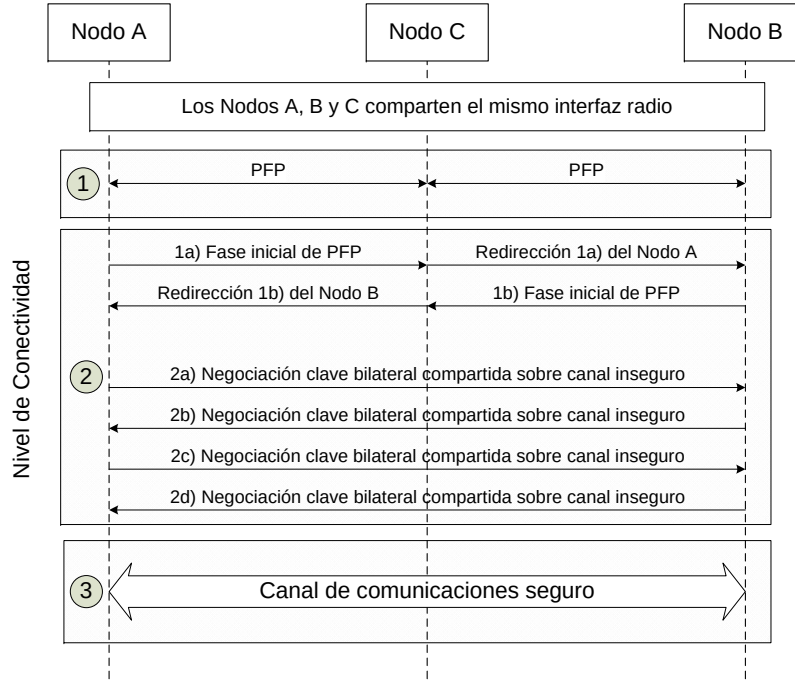


Figura 4.4: Procedimiento de aplicación de la propiedad de transitividad

de criptografía simétrica, que por su velocidad y mejor integración *hardware* son los más adecuados para cifrar los datos intercambiados en las comunicaciones entre dos entidades. Gracias a su uso la latencia y ancho de banda de las comunicaciones se ven mínimamente afectados ante la inclusión de una capa de seguridad.

En la sección anterior se ha introducido el PFP como solución para acordar una clave común entre cada par de nodos personales. A pesar de que un protocolo como el PFP satisface los requerimientos de seguridad de pequeñas redes, existe la necesidad de tener que emplear un PAC cada vez que se empareja un nodo de usuario con el resto, lo que hace que el grado de usabilidad sea bajo en PN de cierto tamaño. Una de las premisas de las PN es dotar al usuario de simplicidad y facilidad de uso de sus nodos. A la hora de definir el PFP los esfuerzos se centraron en diseñar una solución segura y no se tuvieron tan en cuenta los requerimientos de escalabilidad pues, aunque importante en una PN, no se suponía un elevado crecimiento del número de dispositivos. Sin embargo la proliferación de dispositivos de usuarios como teléfonos móviles inteligentes, tabletas o portátiles, en parte originada por la miniaturización y la eficiencia energética, hace que quizás se tenga que replantear el procedimiento de personalización.

El uso de la propiedad de transitividad del PFP ayuda en la personalización de los dispositivos y nodos de usuario, pero en la mayoría de las ocasiones el PAC requiere la interacción del usuario. El número de operaciones a ejecutar siguiendo este procedimiento crece de forma cuadrática $O(n^2)$, siendo más exactamente $\frac{n^2 - n}{2}$ donde n es el número total de nodos en la PN. Si se tiene en cuenta que estas operaciones no son automáticas, se entiende que el PFP no cumple totalmente los requerimientos impuestos por la PN.

En este sentido, parece lógico redefinir el procedimiento de negociación de claves o bien extender el PFP para que sea escalable y apto para funcionar en grandes PN. El renovado procedimiento deberá continuar ofreciendo un alto grado de seguridad, incorporando autenticación y no repudio, al tiempo que incluirá nuevas funcionalidades que faciliten la generación, actualización y revocación de las claves.

La implementación de una PKI es la solución más empleada para constituir asociaciones seguras entre los nodos de un entorno dinámico como el de la PN. Sin embargo, estos mecanismos convencionales de seguridad, privacidad y confianza entre nodos no se pueden aplicar directamente en las PN debido a las condiciones especiales que se imponen. En una PN no se tiene conexión permanente con una TTP y por otro lado el usuario sería bastante reacio a delegar la gestión de seguridad y la confianza entre los nodos de su PN a un tercero por mucha seguridad que éste le proporcione.

Por lo tanto, una solución de compromiso consiste en adaptar la operativa de una PKI a los requerimientos de la PN. Hacer que el usuario sea el responsable de su propia PKI solventaría gran parte de los impedimentos existentes. Esta idea se materializa en lo que se ha denominado PKI Personal, en la cual en lugar de certificados globales emitidos por una TTP, el usuario, a través de su propia CA, emitirá certificados válidos dentro de la PN. Por consiguiente, todos los nodos personales compartirán la clave pública de esta autoridad de certificación de la PN (PNCA, *Personal Network Certification Authority*) como CA raíz de la PN, y serán los certificados emitidos por ella los que sustenten la autenticación entre los nodos y el establecimiento de las claves bilaterales.

Este nuevo protocolo de negociación de claves que extiende las funcionalidades del PFP se denomina protocolo certificado de formación de la PN (CPFP, *Certified PN Formation Protocol*) [150]. Mantiene algunas de las características de PFP como el uso de un PAC para inicializar todo dispositivo personal. Además, como en el caso del PFP, en el CPFP, la característica de personal implica la asociación con otro nodo personal, en este caso la PNCA.

Buscando adaptarse a los escasos recursos de algunos de los potenciales nodos de la PN, el CPFP se apoya en soluciones de seguridad con bajas necesidades de cómputo como la ECC, con la que se logran los mismos niveles de seguridad pero empleando claves más cortas.

El CPFP se lleva a cabo en dos fases. En la primera, todos los dispositivos de la PN se emparejan con la PNCA, adquiriendo un certificado sobre su clave pública con validez a largo plazo y firmado con la clave raíz de la PN. En la segunda etapa, los nodos personales emplean esos certificados como mecanismo de autenticación entre ellos y derivan la clave bilateral compartida mediante algún protocolo *Menezes-Qu-Vanstone* (MQV) [151, 152]. En los estadios iniciales se estableció el empleo del protocolo *Elliptic Curve MQV* (ECMQV) [153]. Posteriormente se consideró que los intercambios planteados presentaban ciertas deficiencias dado que no protegían fiablemente la información privada de la sesión [154], por lo que se recomendó el empleo de soluciones basadas en *Hashed MQV* (HMQV) [155] o *Fully Hashed MQV* (FHMQV) [156]. No obstante, dado que la base de todos estos protocolos de generación de claves de sesión es la misma, el protocolo CPFP no se ve afectado. Su operativa se fundamenta en el uso de dos grupos de claves *Elliptic Curve Diffie-Hellman* (ECDH) públicas y privadas, uno válido a largo plazo y otro efímero. Como

requisito, los extremos deben haber autenticado sus claves de largo plazo, proceso que se lleva a cabo durante la primera fase del CPFP.

4.4.1. Inicialización y personalización mediante la PNCA

La figura de la PNCA se erige como la piedra angular de la seguridad dentro de una PN basada en el CPFP. Se hace difícil imaginar entonces que el dispositivo o nodo que aloje esta funcionalidad no tenga unas características especiales. La principal diferencia entre la PNCA y cualquier otro nodo dentro de la PN es que la PNCA conoce la clave raíz de la PN. Cualquiera que conozca dicho secreto puede ejercer como PNCA, por lo que para evitar comprometer dicha clave, ésta no debe ser almacenada en claro y debe estar cifrada a partir de algún dato o parámetro únicamente conocido por el usuario. No obstante, la tendencia de las personas a elegir claves simples sencillas de recordar y a almacenarlas en cualquier lugar visible [157] sugiere la necesidad de emplear algún elemento adicional que proteja de forma robusta la clave raíz, como pueden ser *tokens* externos o elementos biométricos. En esta línea, las tarjetas inteligentes o dispositivos similares se presentan como los más adecuados para llevar a cabo las tareas de gestión de la PNCA, pues además de aportar robustez en el almacenamiento, implementan mecanismos para auto-bloquearse y auto-destruir la clave en caso de usos malintencionados o ataques. Además pueden conectarse a una gran diversidad de equipamiento como teléfonos móviles en forma de *Subscriber Identity Module* (SIM)), lo que permitirá tener una PNCA fácilmente portable.

El dispositivo que desempeñe las funciones de PNCA debe compartir una interfaz de comunicaciones con el dispositivo que vaya a ser marcado, pues de otra manera no se podría realizar el intercambio de información. En este sentido, el hecho de alojar la raíz de la PNCA en un dispositivo portátil y compatible con múltiples terminales permite intercambiarlo de uno a otro para poder así siempre encontrar un equipo con las características de conectividad requeridas. De todas formas parece lógico que los nodos puente o pasarela sean los más adecuados para actuar como PNCA.

La PNCA se inicializa de forma autónoma generando un par de claves pública y privada *Elliptic Curve Digital Signature Algorithm* (ECDSA) que se emplean para validar la identidad de los nodos personales. La clave pública se asocia a la identidad de la PNCA mediante un certificado autofirmado. Por su parte, cada nodo de usuario realiza una operación similar generando su pareja de claves ECDH pública y privada, que empleará a lo largo de su vida útil.

Dado que el usuario es quien tiene el control sobre el proceso de marcado y determina qué nodos, cuándo y cómo pasan a formar parte de la PN, será él el encargado de comunicar la PNCA con los respectivos nodos o dispositivos. En primer lugar, el usuario tiene que arrancar la PNCA y poner al nuevo dispositivo dentro del rango de alcance de forma que se pueda iniciar el proceso de marcado. Como se ha indicado anteriormente, el dispositivo que aloja la PNCA se selecciona no sólo según sus capacidades en cuanto a seguridad, sino también en función de los medios de comunicación que tenga para poder establecer un PAC con cualquier dispositivo. Típicamente, la autenticación se realiza en proximidad, pudiéndose emplear códigos de barras, tocar el dispositivo (vía NFC) o bien mediante una interfaz de lectura/escritura, en cuyo caso el dispositivo deberá disponer además de teclado y pantalla para interactuar con el usuario.

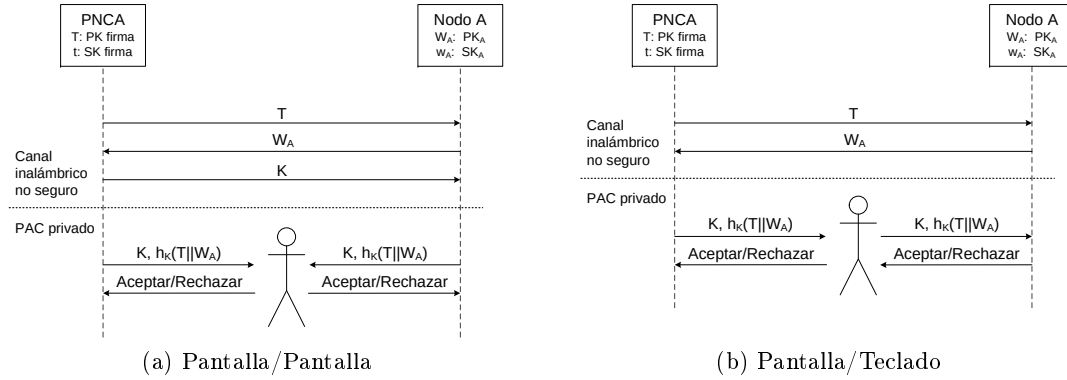


Figura 4.5: CPFP empleando un PAC privado

Una vez que tanto la PNCA como el nodo a personalizar están en el radio de alcance intercambian sus claves públicas a través del canal inalámbrico, normalmente no seguro. Este proceso se autentica por parte del usuario haciendo uso del PAC. Dependiendo del PAC que esté habilitado la participación del usuario será más o menos activa. Para el caso de un PAC privado el usuario será el elemento que transfiera o valide la clave que active la personalización del nodo por parte de la PNCA. En la figura 4.5 se muestran dos escenarios de uso de un PAC privado. En el primero de ellos, el nodo dispone de un teclado a través del cual el usuario introduce la clave que se presenta en la PNCA y valida el resultado de su uso, mientras que en el segundo, el nodo únicamente tiene una pantalla de visualización, por lo que la clave se transfiere por el canal inalámbrico y el usuario valida visualmente que el resultado coincida en ambos dispositivos.

Por su parte, en el caso de ejecutar el procedimiento a través de un PAC público, la PNCA genera un resumen criptográfico a partir de las claves públicas que se transfiere por el canal inalámbrico al nodo. Este calcula el mismo resumen y compara el valor con el recibido. Si ambos valores coinciden notifica al usuario de alguna forma que la transferencia se ha realizado correctamente para que sea él quien en última instancia dé el visto bueno a la personalización. En la figura 4.6 se describe este escenario. Reseñar que en el caso de usar un PAC público el usuario confía en que el nodo esté ejecutando correctamente los algoritmos, al igual que acepta que la función de resumen empleada es robusta para la detección de modificaciones, lo que con una elevada probabilidad asegura el proceso frente a ataques de suplantación de identidad.

Como resultado de estos intercambios, la PNCA emite un certificado de la PN asociado a la clave pública del nodo. Este certificado es el que dota al nodo de la característica de personal y establece el medio mediante el cual su identidad podrá ser verificada por cualquier otro miembro de la PN, lo que permitirá la generación de las claves bilaterales compartidas a largo plazo y, por tanto, el establecimiento de la relación de confianza mutua. El certificado personal tendrá validez mientras no se supere su fecha de expiración (fijada por la PNCA) o la PNCA lo revoque por haber sido comprometido el nodo. En cualquiera de estos casos, se rescinde la relación de confianza con el resto de los nodos personales, pues el nodo cuyo certificado no sea válido deja de pertenecer a la PN y pierde su condición de personal.

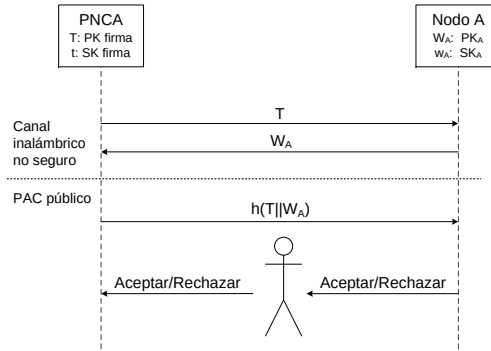


Figura 4.6: CPFP empleando un PAC público

El certificado personal vincula la identidad del nodo en la PN con su clave pública. Hasta ahora se ha fijado la identidad a partir de características inmutables de las interfaces de red (p. ej. la dirección MAC) que siempre forman parte del nodo. Por otro lado, también se ha comentado que los usuarios pueden no querer realizar esa asociación. El CPFP abre una nueva posibilidad. La clave pública ECDH es una buena candidata a servir de semilla para generar la identidad del nodo. Por su característica de invariante durante la vida del nodo, la identidad se podría determinar a partir de un resumen de esta clave. En caso de tener que revocar la clave, implicaría también un cambio en la identidad del nodo, lo que en cierta manera incrementa la seguridad al evitar el riesgo de reemplazo de identidad. Puesto que la validez de la identidad de un nodo personal está circunscrita a los límites de la PN, la decisión final de qué procedimiento emplear la tiene el propio usuario como dueño de su PN.

En todo caso, para facilitar la identificación del nodo por parte del usuario, el usuario debe seguir asignando a todos sus nodos un nombre corto y fácil de usar que vaya también incluido en el certificado personal.

La personalización de los n nodos de una PN supone que el usuario, a través del PAC, debe actuar n veces. El número de operaciones que el usuario debe ejecutar en esta fase es, por tanto, $O(n)$.

4.4.2. Generación de las claves bilaterales compartidas a largo plazo

El empleo de certificados digitales es uno de los métodos más implantados para definir la confianza en la identidad de sujetos o equipos en las redes de comunicaciones. Un certificado vincula la información de identidad de una entidad con su clave pública, ligada también a su clave privada, lo que permite validar las transacciones en las que está inmersa esa entidad.

En esta segunda y última etapa del CPFP los nodos personales se valen de sus certificados personales y de la dupla de claves pública y privada de largo plazo para derivar la clave bilateral compartida de largo plazo. Para ello se emplea un protocolo basado en MQV. La ventaja de los protocolos de la familia MQV frente a los ECDH es que incluyen funcionalidades que proporcionan una mayor resistencia ante posibles riesgos de reemplazo de clave o identidad. Estos protocolos aseguran una autenticación fuerte y evitan que un

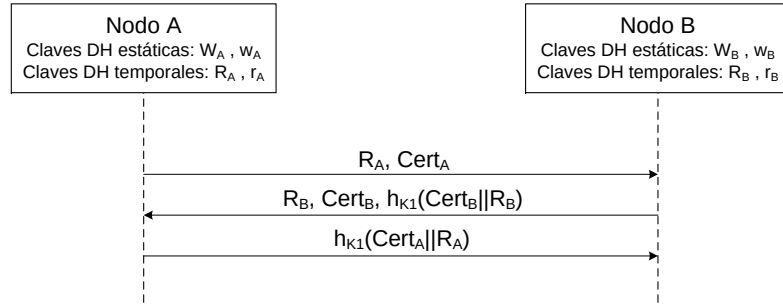


Figura 4.7: Proceso de derivación de las claves bilaterales compartidas a largo plazo

tercero pueda enmascarar la comunicación y comprometer la clave bilateral que se genere. Adicionalmente, como se ha insistido, el uso de metodologías basadas en curvas elípticas disminuye la sobrecarga computacional, es simétrico en su operativa (los nodos pueden intercambiarse y el resultado se mantiene) y no requiere ni cifrado ni sellado de tiempo para asegurar los intercambios de datos. Es por ello que estos procedimientos, principalmente FHMV, son ideales para procesos de negociación de claves eficientes [151, 158, 159].

En la figura 4.7 se resume esta etapa, donde se emplea la negociación en tres pasos del protocolo FHMV [156], que incluye confirmación de clave, para determinar la clave personal $K_{PN}(A, B)$. El protocolo opera de la siguiente manera:

1. El nodo A genera una pareja de claves temporal (r_A, R_A) y transmite la clave pública temporal R_A junto con su certificado estático $Cert_A$ a B
2. En recepción, el nodo B:
 - Verifica la validez de los datos recibidos y genera su propia pareja de claves temporales (r_B, R_B) .
 - A partir de todos los datos disponibles y empleando dos funciones de generación de claves KDF_1 y KDF_2 , deriva dos claves K_1 y K_2 [156].
 - Calcula el código de autenticación $t_B = h_{K_1}(R_B || Cert_B)$.
 - Remite $R_B, Cert_B$ y t_B a A.
3. A la recepción del mensaje, el nodo A:
 - Verifica la validez de los datos recibidos.
 - A partir de todos los datos disponibles y empleando dos funciones de generación de claves KDF_1 y KDF_2 , deriva dos claves K_1 y K_2 y chequea t_B .
 - Calcula el código de autenticación $t_A = h_{K_1}(R_A || Cert_A)$.
 - Remite t_A a B y da por válida K_2 como $K_{PN}(A, B)$.
4. El nodo B recibe y valida la información dando por válida K_2 como $K_{PN}(A, B)$

Gracias al procedimiento impuesto por el CPFP, el usuario no tiene que interactuar para establecer las relaciones de confianza entre sus nodos. Una vez que los nodos personales se

detectan y se ponen en contacto, usualmente gracias a los mensajes de difusión emitidos por el módulo de descubrimiento de vecinos, el proceso de autenticación y negociación de claves se lanza de forma automática. Ésta se puede considerar la principal diferencia sobre el anterior modelo basado en el PFP, en el cual el emparejamiento de los dispositivos se hacía de forma manual.

Valiéndose del CPFP, el número de operaciones que deben ser ejecutadas para establecer la relación de confianza entre todos los nodos en una PN compuesta por n nodos es de $\frac{n^2 + n}{2}$. Sin embargo, aunque en orden coinciden con las del antiguo PFP, en este caso $\frac{n^2 - n}{2}$ se realizan de manera automática, por lo que la implicación del usuario se ve reducida notablemente. Se puede concluir entonces que el CPFP globalmente es un protocolo $O(n)$ en cuanto a carga para el usuario y, por tanto, es más adecuado que el anterior PFP para PN de medio o gran tamaño.

Además, el CPFP aporta aún más ventajas sobre el PFP. En el CPFP la confianza se sustenta en la PKI personal, lo que facilita la aplicación de la propiedad de transitividad, pues las relaciones de confianza extremo a extremo se pueden construir sobre la confianza en los certificados emitidos.

Por otro lado, se ha mencionado la posibilidad de revocar la pertenencia a la PN de un nodo personal. Si por cualquier causa un nodo se ve comprometido, el PFP no presenta ningún mecanismo que facilite la rescisión de la confianza del resto de los nodos con él. En cambio el CPFP, al extender los mecanismos tradicionales de revocación de una PKI, sí facilita la supresión de la afiliación del nodo a una PN. Ésta es otra de las nuevas funcionalidades que proporciona el nuevo CPFP y que se describe a continuación como parte de las extensiones a los mecanismos básicos desarrolladas durante el trabajo en esta tesis.

4.4.3. Revocación de pertenencia a la PN

Un certificado relaciona la identidad de una entidad con sus claves criptográficas, siendo una TTP quien legitima la veracidad de dicha relación. Gracias a esta TTP, que garantiza ese vínculo, otros aceptan como válida la información alojada en ese certificado. Una PKI no es más que la infraestructura en la que se apoya esa TTP para generar el entramado de confianza. Dentro de la PKI la entidad que se encarga de verificar las credenciales y emitir los certificados se denomina CA. La confianza en esa CA se extiende directamente a los certificados que emite.

La vigencia de esos certificados está limitada temporalmente por la CA, donde el período dependerá de las políticas de emisión de dicha CA. Dicho de otro modo, la CA garantiza que el vínculo presentado en el certificado es aceptable durante un tiempo, fuera del cual no se compromete a avalarlo. A partir del momento en que la CA deja de respaldar la información incluida en el certificado, se considera que dicho certificado ha sido revocado. No obstante, un certificado puede ser revocado no sólo por haber alcanzado su fecha de caducidad, sino que también puede ser revocado por haberse emitido de forma incorrecta o porque las claves o información asociada se hayan visto comprometidas [160, 161]. En todos los casos, la confianza en dicho certificado deja de existir.

Por tanto, validar un certificado ya no sólo implica ratificar la confianza en la entidad emisora, sino que además hay que comprobar la validez de éste y confirmar que no haya sido revocado. Una PKI dispone los medios para determinar la validez de un certificado basándose en su lista de certificados revocados (CRL, *Certificate Revocation List*). Estas listas contienen los registros de los certificados que, habiendo sido emitidos por una CA o varias CA, están invalidados. Normalmente se identifican los certificados a partir de su número de serie, único dentro del ámbito de una CA.

Las CRL deben ser periódicamente actualizadas y distribuidas a todos los elementos de la red, pues incorporan información de seguridad muy sensible. En [162] se puede encontrar una perspectiva general de diferentes esquemas de revocación, aunque lo más común es albergar la CRL en un servidor central. Independientemente del esquema de CRL que se emplee, una CRL es siempre incremental, pues en caso de querer readmitir a una entidad, no se reinstaura la validez del certificado previamente revocado, sino que la CA emite uno nuevo, es decir, todo certificado es irreversiblemente revocado.

La PKI personal debe extender todas estas funcionalidades en una PN, donde ahora el usuario es quien deposita la confianza en sí mismo en lugar de en un tercero. La figura de la PNCA como emisora de certificados personales basándose en el CPFP ya ha sido introducida, pero la definición y puesta en conocimiento de una lista negra o registro de nodos que han perdido su condición de personales es un aspecto aún más importante si cabe que el hecho de incorporar nuevos nodos personales. Tanto es así que un dispositivo cuya integridad esté comprometida, si no se dispone lo contrario, sigue teniendo acceso a todos los recursos y servicios de la PN, lo que implica un gran riesgo de seguridad.

En su PN el usuario ostenta la potestad de incluir nuevos nodos al tiempo que también debe gestionar la validez de la pertenencia a dicha PN. Cada vez que un nuevo nodo pasa a formar parte de la PN, la lista de miembros se actualiza con la información de ésta (identificador, etc.). Del mismo modo, cada vez que se revoca un certificado asignado a un nodo personal, la PNCA debe actualizar el fichero de CRL con la información que identifique dicho nodo. La información mínima a incluir es:

- Identificador único del nodo.
- Número de serie del certificado asociado revocado.
- Sello de tiempo y/o versión de CRL.
- Información complementaria describiendo las razones de la revocación.

La lista de miembros y la CRL de una PN están estrechamente relacionadas, pues los registros de una no deberían estar reflejados en la otra. Puede darse la situación que un nodo que hubiera sido comprometido recupere su estado de nodo personal. Para ello el nodo deberá presentarse nuevamente ante la PNCA, quien lo dotará de nuevas credenciales personales.

Puesto que debe ser distribuida al resto de nodos de la PN, la CRL es además firmada empleando la clave privada de la PNCA (SK_{PNCA}) para garantizar la integridad, autenticidad y no repudio de la información en ella contenida. Así, cada nodo podrá comprobar

la validez de este listado mediante la clave pública de la PNCA (PK_{PNCA}) obtenida durante el procedimiento de marcado. Con esta operativa se evita que ningún nodo pueda ser revocado de forma ilícita.

En cada operación de revocación, la PNCA actualiza el número de versión y/o refresca el sellado de tiempo. La operativa dentro de la PN se simplifica empleando el número de serie, pues se evita tener que mantener todos los nodos sincronizados.

Es tras cada revocación cuando la CRL se tiene que distribuir a todos los nodos de la PN, si bien existen esquemas de distribución periódicos. La efectividad en el uso de la CRL se obtiene siempre y cuando se asegure que en un momento dado cualquier nodo de la red dispone de la versión de CRL más actual, ratificando que la relación de confianza entre dos nodos cualesquiera sigue vigente. Idealmente y en aras de reducir el volumen de datos que circula por la red, dado que la CRL tiene carácter incremental, únicamente se transmitirán los cambios entre la versión actual y la anterior.

La validez de una CRL, como la de los certificados, viene impuesta por las políticas que defina su CA responsable. En el caso de la PN, se rige por los requerimientos que imponga el usuario. Es él quien realmente conoce la validez temporal de su CRL, pues es quien la gestiona. Incluso puede señalar ciertas versiones de su CRL como más relevantes considerando los nodos que se incluyan en las actualizaciones. En principio, la PN se puede considerar una red cuya tasa de actualización en expansión no es muy alta, y del mismo modo se puede considerar la tasa de eliminación de nodos personales. En base a esto, no se considera prioritaria la tarea de actualizar periódicamente la CRL de los nodos personales, pero sí notificar los cambios más notables a consideración del usuario. No obstante, sea corta o larga la validez de la CRL, sus actualizaciones tienen que ponerse a disposición de los nodos personales lo antes posible.

El proceso de distribución de la CRL se puede llevar a cabo de muy diversas maneras en una PN, todas ellas, al igual que se ha venido insistiendo con otros procedimientos, no basadas en una única entidad central. Por las características de la PN la solución debe ser distribuida y funcional tanto en entornos conectados (*online*) como desconectados ad-hoc (*offline*). Se busca con ello reducir la necesidad de tener que acceder a la PNCA como entidad central poseedora de la versión más actual.

En este sentido una posibilidad es emplear la SCMF como entorno de publicación, distribución y acceso bajo demanda a la información de seguridad. Esta aproximación presenta la ventaja de que no se requiere implementar módulos, ni servicios, ni interfaces adicionales. Si bien la SCMF es una de las opciones más adecuadas para hacer disponible la información, la información de seguridad alojada en la CRL quedaría enmascarada como información de contexto, aspecto éste poco óptimo dado el especial tratamiento que ésta debería tener. En este sentido, a pesar de que la integridad y autenticidad de la CRL se acredita a través de la firma de la PNCA, el tratamiento por parte de la SCMF podría generalizarse a obtener información puntual de un único nodo en lugar de distribuir completamente la CRL con lo que la veracidad de la información podría ser puesta en duda.

La información de la CRL entra en liza en el momento en que los nodos se descubren y quieren emparejarse bien a largo plazo o de forma temporal para comunicarse. Esos procesos son usualmente espontáneos y de duración muy corta, por lo que la latencia de la operación

debe ser lo más reducida posible. Son todos los nodos por igual los que participan, con capacidades SCMF y sin ellas, por lo que las necesidades de la SCMF no se ajustan a los requerimientos de la CRL. Sin embargo, por cuestiones de optimización de procedimientos y toma de decisiones de contexto, sí se considera interesante y recomendable disponer de una réplica de la CRL alojada en las bases de datos de la SCMF.

Se presentan a continuación dos opciones para distribuir de manera eficiente la CRL basadas en el nivel de conectividad y red implementados en todos los nodos y dispositivos de la PN; una de ellas se sustenta en ciertos nodos de los *clusters* como puntos de distribución y otra totalmente descentralizada considerando un entorno ad-hoc P2P.

4.4.3.1. Distribución de CRL jerarquizada

Considerando la manera en la que se organiza la PN, parece claro pensar que dentro de los diferentes *clusters* sean los nodos pasarela o *gateways*, como nodos conectados con el exterior, los que tendrán acceso a la información de seguridad más actualizada independientemente de la localización de la PNCA. Por tanto, al iniciar el proceso de distribución de la CRL, es lógico considerar a estos nodos como los puntos de distribución. Así, en aquel *cluster* en que se encuentre la PNCA, el nodo pasarela correspondiente remitirá la lista más actualizada al resto de los *clusters* a través de los túneles seguros previamente establecidos. De igual manera, cualquier cambio en la lista de revocación se propagará, actualizando la disponible en los demás *clusters*.

Se podría plantear incluso que el agente de la PN disponga de una copia de la versión más actual de la CRL. Del mismo modo que los nodos pasarela distribuyen la CRL entre sí, sería sencillo redirigirla al agente de la PN. En esta situación, la PN asemejaría la operativa de una PKI tradicional en cuanto a la gestión de la CRL, delegando la responsabilidad de la CA en el agente de la PN. No obstante, se considera que esta opción es una vuelta atrás, ya que toda la funcionalidad se centra en disponer de una entidad central permanentemente accesible.

Dentro de cada *cluster*, excepto en el que se encuentre la PNCA, la información más actualizada de revocación se encontrará en estos nodos pasarela. Esta información se difundirá entre los nodos personales haciendo uso de los mecanismos de comunicación segura existentes dentro del *cluster*. Aunque dada la temporalidad de la PN las actualizaciones de CRL no serán frecuentes, se recomienda implementar algoritmos de inundación controlada para publicar las nuevas CRL, evitando en la medida de lo posible la sobrecarga de la red.

No obstante, pueden existir *clusters* que no hayan estado conectados por un tiempo y por tanto sus nodos pasarela no hayan recibido actualizaciones. En este sentido, dado que los nodos personales tienen libertad para pasar de un *cluster* a otro, los nodos provenientes de otros *clusters* (en *roaming*) podrán disponer de información más actualizada en función de las condiciones del *cluster* de donde provengan y el *cluster* destino. En estos casos, cuando los nuevos nodos se presenten en el nuevo *cluster*, propagarán la nueva versión de la CRL si es que es más actual que la existente.

Aunque ésta es una solución viable para una gestión distribuida de la CRL en el caso que todos los *clusters* estén o hayan estado conectados, no hay que olvidar el hecho de que los *clusters* en una PN se generan espontáneamente creando redes puramente ad-hoc. En

muchos de esos casos los nodos pueden no haber estado conectados ni con nodos pasarela, ni mucho menos con la PNCA durante mucho tiempo. Es, por tanto, necesario definir un procedimiento para intercambiar la información de CRL en entornos completamente P2P.

4.4.3.2. Intercambio P2P de CRL

Por definición, todos los nodos de un usuario para formar parte de su PN han tenido que ser marcados como tales. Al finalizar el proceso CPFP, en el que la PNCA valida la identidad de dichos nodos y los convierte en personales, la PNCA transfiere la CRL más actualizada (figura 4.8). A partir de ese momento, en un entorno ad-hoc, a no ser que el nodo se encuentre dentro del radio de alcance de la PNCA, deberá confiar en el resto de los nodos personales para obtener actualizaciones del listado de nodos personales confiables.

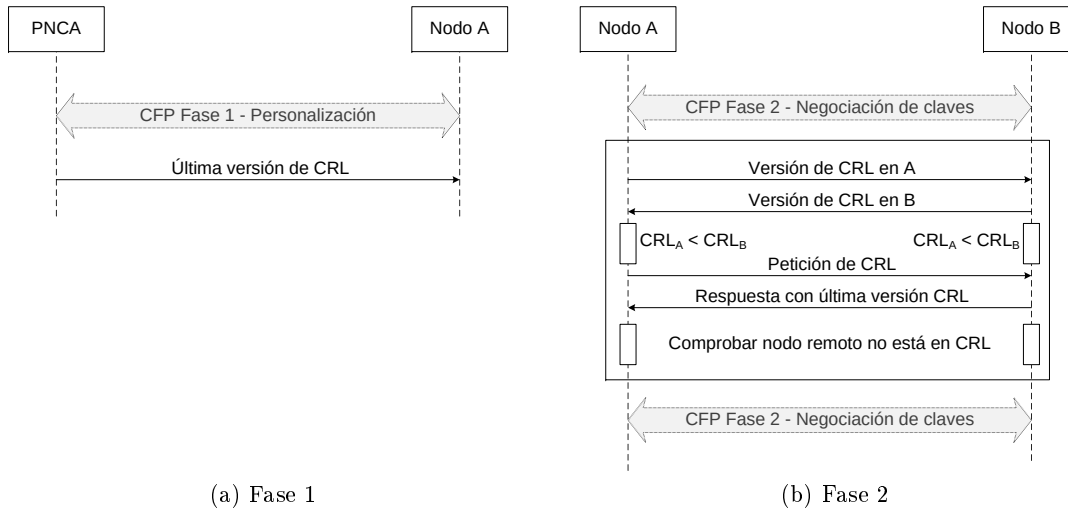


Figura 4.8: CPFP con intercambio de CRL

Dos nodos personales cualesquiera que se vayan a comunicar dentro de la PN, según lo establecido en la segunda etapa del CPFP, deben comprobar la validez de sus identidades y derivar sus claves bilaterales compartidas. La modificación de esta etapa incluyendo la validación del CRL se muestra en la figura 4.8. Como primer paso verificarán, mediante sus CRL, que el otro extremo sigue siendo un nodo personal, tras lo cual procederán a generar las claves bilaterales que reflejen la relación de confianza mutua.

Dado que los nodos han podido ser marcados en momentos temporales diferentes, es muy probable que dispongan de distintas versiones de CRL. En este punto se plantean dos opciones: actualizar la CRL tras la finalización de esta etapa del CPFP o de forma previa. En un principio, parece natural que se realice al finalizar para garantizar la seguridad del intercambio y cerciorarse ambos nodos de que son personales y no se han visto comprometidos. Sin embargo, no hay que olvidar que la CRL está firmada por la PNCA, cuya firma no puede ser suplantada. Esto garantiza la integridad y validez de la CRL incluso aunque los nodos hayan sido comprometidos. Pese a esto, los nodos comprometidos pueden elegir intercambiar una CRL más vieja que la última que dispongan, aunque en ocasiones puede que incluso esa CRL sea más nueva que la que almacene el otro extremo. Ambas

opciones son igualmente válidas, siendo la decisión final del implementador de la PN, si bien posponer el intercambio a la finalización del CFP permite que la CRL se intercambie a través de un canal inalámbrico seguro. En la figura 4.8 se representan ambas opciones.

Tras personalizarlos, los nodos mantienen una comunicación casi constante dentro del *cluster* al que pertenecen, lo que ofrece una nueva oportunidad para propagar la CRL. Como se describió en el apartado 3.4, cuando dos nodos personales se encuentran se descubren a partir de los *beacons* que están difundiendo. Como paso previo a entablar una comunicación entre ellos, establecen un canal seguro y autenticado a partir de las claves bilaterales de largo plazo. Antes de iniciar esa sesión segura ambos nodos se cercioran que el otro extremo sigue siendo confiable, para lo que comprueban que el otro extremo no está incluido en la CRL. Los mensajes de difusión contienen información de la identidad de los nodos que puede ser cruzada con la incluida en la CRL. Esta verificación previa permite eliminar el riesgo de establecer una sesión con un nodo que haya sido comprometido y exponer información sensible.

Como se describe en la siguiente sección, una vez que ambos nodos se han autenticado y reconocido como personales, se lanza un proceso de negociación de claves, del cual resulta una clave de sesión válida entre los dos nodos que cifra el canal de comunicaciones temporalmente. La CRL se puede intercambiar antes o sobre el canal inalámbrico seguro conociendo las ventajas e inconvenientes que ya se han descrito anteriormente. La figura 4.9 permite ilustrar gráficamente el procedimiento.

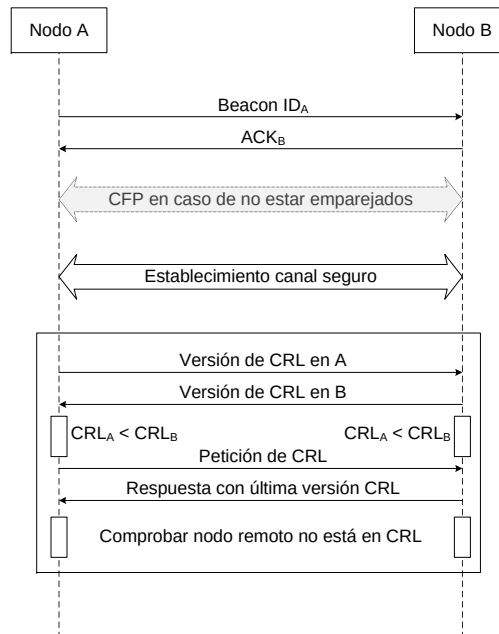


Figura 4.9: Protocolo de autenticación y securización del canal con intercambio de CRL

Siempre que un nodo obtenga una CRL más actual, propagará esa información a los vecinos con los que tenga establecida una sesión segura. No obstante, centralizando la distribución en los nodos pasarela se logra un mayor control del proceso de inundación y se evita la sobrecarga del *cluster*.

A la recepción de una nueva versión de la CRL, cada nodo debe analizar las sesiones que tiene activas. Todas aquellas que incluyan nodos que han sido revocados deberán interrumpirse, dado que la relación de confianza no está ya vigente. No hay que olvidar que el tráfico de difusión también se encuentra securizado en la PN. Dado que un nodo emplea la misma clave de sesión de difusión para comunicarse con todos sus vecinos, al haber distribuido dicha clave a un nodo que ya no es personal, para mantener la seguridad del canal de comunicaciones, la clave de difusión tendrá que ser refrescada y redistribuida a través del canal punto a punto seguro de comunicaciones que mantiene durante la sesión con sus vecinos.

Los procedimientos descritos en esta sección ayudan a disponer de la versión más actual de la CRL de la PN en entornos puramente ad-hoc. El uso de las CRL tiene valor si todos los nodos en algún momento tienen la última versión de ésta. La homogeneidad de las CRL disponibles en los nodos personales permite mantener la robustez de la PN, evitando los usos malintencionados de nodos considerados personales.

4.4.4. Resiliencia de la PNCA

El papel de la PNCA como piedra angular de la seguridad de la PN supone que sobreponerse ante incidencias inesperadas sea algo delicado por el impacto que ello conlleva sobre la PN. Circunstancias tales como que la PNCA no esté disponible o que su seguridad se haya visto comprometida no pueden suponer que se tengan que posponer o incluso abandonar la personalización de nodos u otras acciones sobre la PN. Aunque es difícil que al usuario se le presente esta coyuntura si opera siguiendo unos parámetros de seguridad mínimos, se deben proporcionar los mecanismos para evitar estos problemas e incluso recuperarse.

Hasta el momento la PNCA se ha identificado más como una funcionalidad que como un nodo en sí. La única diferencia entre cualquier nodo personal y la PNCA es que este último conoce la clave secreta de la PN SK_{PNCA} . Esto significa que cualquier nodo que conozca este secreto puede ejercer de PNCA. Por tanto, parece factible el considerar alojar la SK_{PNCA} en un dispositivo o token portátil y robusto que permita al usuario conectarlo a diferentes terminales, en cualquier momento y situación. La clave se almacenará cifrada, empleando un secreto fuerte, para evitar que cualquier atacante tome control de la PN en caso de que se extravíe la PNCA.

Al poner en funcionamiento la PNCA, la clave de la PN en claro se mantendrá en la memoria del dispositivo por un tiempo limitado. No obstante, es recomendable que el dispositivo seguro o token que la aloje sea capaz de realizar todos los algoritmos impuestos por el CPFP de manera autónoma, evitando así que la SK_{PNCA} tenga que ser compartida con el huésped que ejecute la PNCA. A lo largo del documento ya se ha señalado a las tarjetas inteligentes como uno de los dispositivos más adecuados para almacenar el secreto de la PN.

El token puede no disponer de la memoria suficiente para alojar el listado de todos los certificados personales emitidos y revocados. En ese caso, este listado se almacenará firmado en los diferentes nodos que ejerzan de PNCA. Será responsabilidad del usuario transferir o poner en contacto a todos estos nodos para sincronizar las listas locales y proporcionar una funcionalidad completa.

Todas las medidas extraordinarias que se implanten para mantener la PNCA no evitan que en caso de extravío haya que re-personalizar todos los nodos de la PN, pues si la raíz de confianza ya no es fiable, tampoco lo pueden ser los nodos personales.

4.5. Seguridad multicapa

Hasta ahora las descripciones de la arquitectura de seguridad se han centrado principalmente en cómo convertir un nodo en personal dando por sentado que toda vez que un nodo es parte de la PN y mantiene una relación bilateral con el resto de los nodos de ésta la seguridad está garantizada. No obstante, el alto grado de seguridad definido como relación de confianza entre los nodos debe ser extensible a las comunicaciones que establezcan en cada una de las capas de abstracción definidas y/o niveles de la pila de protocolos de comunicaciones. Es necesario consolidar soluciones que permitan extender la operativa con las claves bilaterales buscando no exponerlas en los intercambios entre nodos.

La implantación de la filosofía de considerar la PN como una PKI personal, gracias a la PNCA, proporciona una mayor flexibilidad y notables mejoras sobre la primera opción de personalización de los nodos basada en el PFP. Sustentado en el CPFPP, se incrementa el grado de automatización de los procedimientos y se logra ampliar el soporte a los requerimientos de seguridad planteados desde un inicio.

El CPFPP se apoya en la criptografía asimétrica para negociar y distribuir claves bilaterales entre los nodos que operarán sobre algoritmos de criptografía asimétrica. Se definen, por tanto, dos niveles dentro de la PN: uno basado en la PKI personal que permite identificar con garantías los nodos personales y otro basado en la clave bilateral simétrica que, además de fijar la confianza mutua entre nodos, es la base para asegurar las comunicaciones entre ellos.

La clave bilateral compartida de largo plazo acelera la creación y la operación del canal de comunicaciones seguro. Sin embargo, esta clave no debería usarse directamente ya que un agujero de seguridad en los algoritmos o procedimientos podría dar a conocer esta clave y destruir la confianza entre los nodos y, por ende, la PN.

Para no comprometer dicha clave se plantea, como parte de este trabajo, una estructura de claves multinivel derivadas a partir de la clave bilateral compartida de largo plazo, es decir, los nodos generan dinámicamente una clave bilateral en cada capa (conectividad, red, etc.) válida sólo para las relaciones entre pares de nodos y que salvaguarda la comunicación en ese nivel específico. Servirse de claves independientes para cada nivel asegura que en caso de que una se vea comprometida el sistema completo no se resiente. El resto de los niveles de seguridad sirven de respaldo para mantener una comunicación segura si bien podría, de mutuo acuerdo entre los nodos, volverse a generar una nueva clave en el nivel violado.

La propia heterogeneidad de soluciones y tecnologías empleadas en cada capa conlleva un incremento de la granularidad en el tratamiento de la seguridad; cada tecnología de comunicación radio emplea sus propios algoritmos de seguridad, por ejemplo *Wi-Fi Protected Access* (WPA) o *Wired Equivalent Privacy* (WEP) para interfaces IEEE 802.11, el número de identificación personal (PIN, *Personal Identification Number*) en Bluetooth, etc.; cada solución de seguridad de nivel de red emplea sus propios protocolos como IPSec, etc.; cada

aplicación se autentica o cifra sus datos e intercambios de forma diferente empleando SSL, Kerberos [163] u otras alternativas. Este escenario supone que se deben extender las claves definidas para cada nivel dependiendo del uso o tecnología a la que se oriente. Es más, cada sesión entre nodos debería emplear una clave temporal derivada ex profeso.

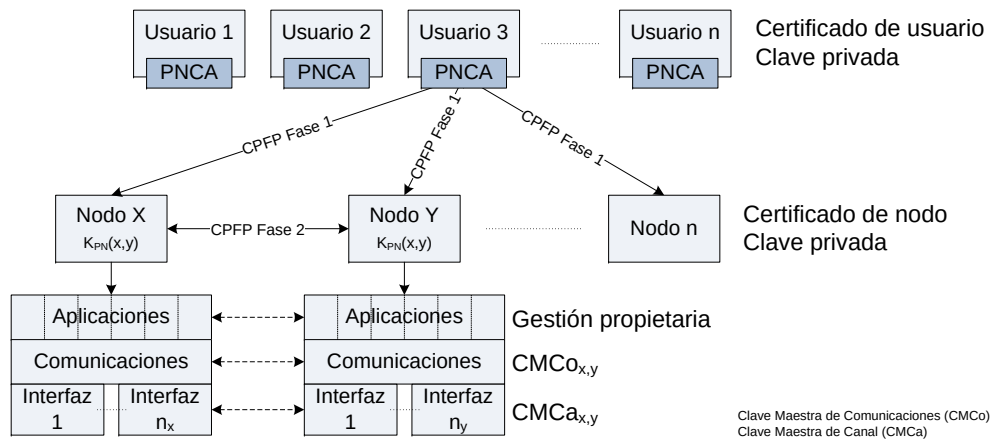


Figura 4.10: Jerarquía de derivación de claves en una PN

La figura 4.10 refleja la cadena de validación y herencia de claves dentro de un nodo y entre cualquier par de nodos de la PN. A partir de la clave bilateral compartida a largo plazo, obtenida tras la segunda etapa en el CPFP, los nodos, empleando datos conocidos por ambos, bien sean los identificadores del servicio, las direcciones de nivel de red o las de cada interfaz de red, y aplicando sobre ellos procedimientos criptográficos derivarán las claves bilaterales propias de cada nivel. Su uso, unido a la generación de claves de sesión propias de cada capa, evita poner en riesgo la relación de confianza entre los nodos. La figura 4.11 resume lo anteriormente expuesto.

4.5.1. Seguridad a nivel de enlace

Dentro de una PN el canal de comunicaciones entre dos nodos es único y se descompone en varios subcanales, que dependerán del tipo de interfaz que se emplee para la transferencia entre los nodos. La UCL, a través de su AdP de gestión de seguridad, trata de ocultar y superar las deficiencias que puedan existir en los diferentes canales radio. Además, las características propias de cada canal radio hacen que, desde el punto de vista de operativa de seguridad, el funcionamiento difiera de unos a otros. En este sentido, dicho módulo de seguridad en colaboración con la CdA ofrece un modo de operación global y homogéneo por encima de la seguridad inherente a cada tecnología que posibilita la automatización y mejora de los procesos de seguridad subyacentes.

Bien durante la negociación de la clave K_{PN} o bien en el momento en que los nodos se descubren con la voluntad de comunicarse, se dan a conocer las interfaces de nivel de enlace de que cada uno dispone. La intersección entre aquellas disponibles en los nodos serán las habilitadoras del canal de comunicación entre ellos.

Para cada posible canal de nivel de enlace los nodos derivan una clave bilateral a la que

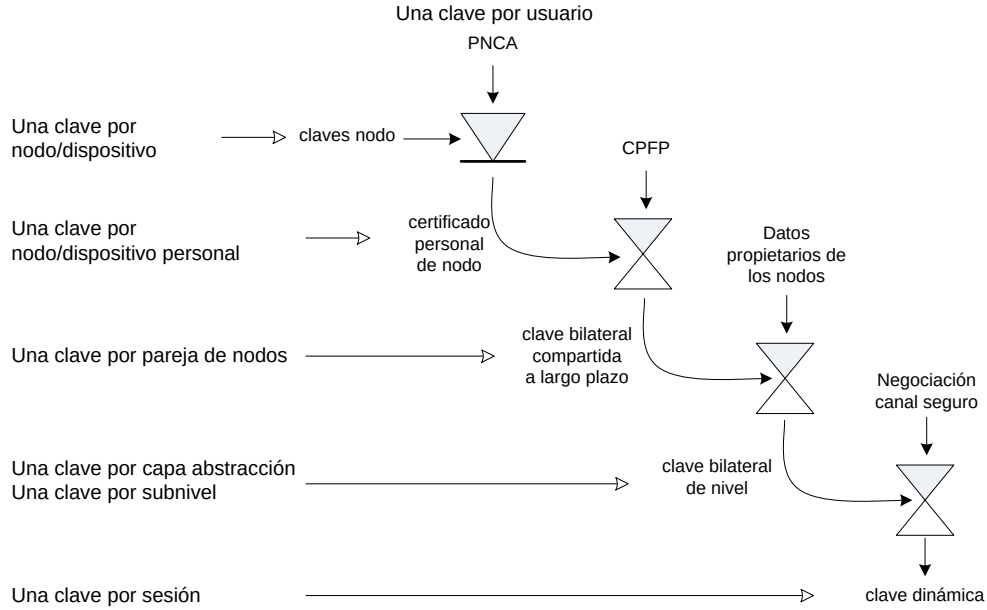


Figura 4.11: Proceso de derivación de claves en una PN

se denomina Clave Maestra del Canal (CMCa), cuyo cálculo se rige por

$$\text{Clave Maestra de Canal (CMCa)} = h_{K_{PN}}(\text{MAC}_1 \parallel \text{MAC}_2 \parallel \text{Tipo de Canal})$$

donde

- MAC_x es la dirección MAC de los nodos.
- Tipo de Canal es un valor dependiente del canal radio empleado (WiFi, Bluetooth, GPRS, UMTS, etc.).
- $h_k(m)$ es la operación resumen para generar una clave de longitud fija.

Esta clave se emplea nuevamente para diversificar y obtener claves de sesión temporales con las que cifrar y autenticar cada mensaje que se intercambie entre los nodos. El procedimiento de generación de estas claves y la longitud de las mismas dependerán de las capacidades de cómputo de los dispositivos y del propio canal. De forma genérica se define que la negociación se realizará empleando un intercambio *Extensible Authentication Protocol* (EAP) [164, 165] que se iniciará una vez que un nodo detecte la presencia de un nuevo vecino mediante los mensajes de difusión o *beacons*. La recepción de un *beacon* supone que ambos nodos usan el mismo tipo de interfaz de comunicaciones radio y la clave temporal que se derive tendrá validez sólo para su uso a través de ese canal radio.

En la figura 4.12 se muestra el intercambio a tres bandas a partir del cual los nodos generan la clave de sesión temporal y comparten sus claves de difusión. El detalle del formato de los paquetes intercambiados se encuentra disponible en [101]. Para las operaciones de cifrado simétrico se recomienda emplear *Advanced Encryption Standard* (AES) [166] con

una clave de 256 bits, por ser un algoritmo con un alto rendimiento. El proceso se desglosa en las siguientes etapas, siendo B_X la clave de difusión del nodo X y T_X un marcado de tiempo para incrementar la aleatoriedad:

1. El nodo A recibe un *beacon* del nodo B.
2. El nodo A envía una petición EAP:

$$\text{EAP Request}(E_{CMC_{a_{AB}}}(ID_A \| N_A \| B_A \| T_A))$$

3. El nodo B responde con un mensaje EAP:

$$\text{EAP Response}(E_{CMC_{a_{AB}}}(ID_B \| N_A \| B_A \| N_B \| B_B \| T_B))$$

4. Si la comprobación es exitosa, el nodo A responde:

$$\text{EAP Success}(E_{CMC_{a_{AB}}}(ID_A \| N_B \| T_B))$$

5. El nodo B valida el intercambio.

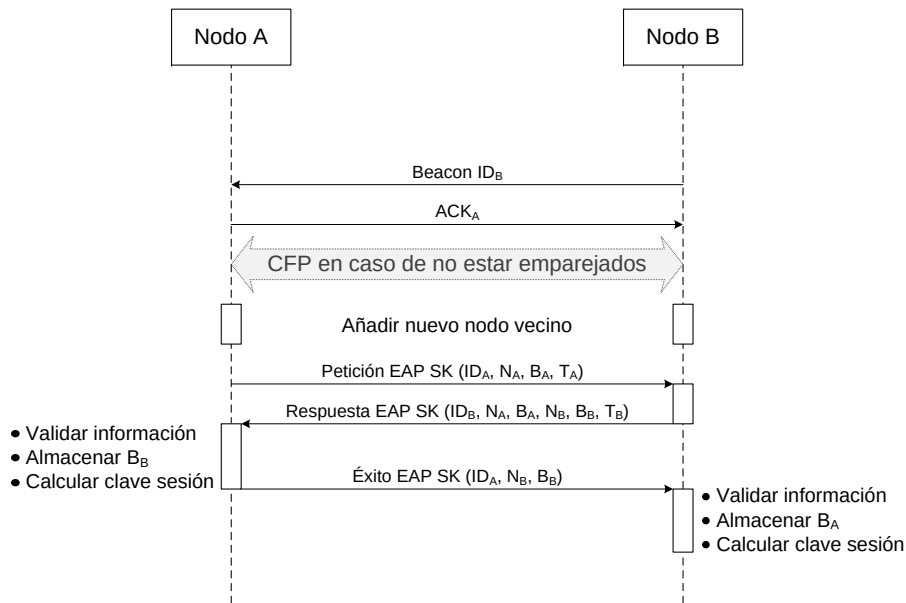


Figura 4.12: Derivación de claves de sesión a nivel de enlace

Hay que incidir nuevamente en que esta negociación sirve también para intercambiar las claves que empleará cada nodo para cifrar y autenticar los mensajes de difusión. La clave de difusión la decide de forma unilateral cada nodo y el resto de los nodos personales únicamente la usarán para descifrar y validar los mensajes recibidos. En aquellos canales que no implementen procedimientos de difusión, la propia UCL puede emular ese comportamiento o bien delegar en las capas superiores.

Las claves de sesión generadas se emplean para proteger un canal en particular, lo que implica no sólo cifrar los mensajes transmitidos, sino también autenticar el origen de éstos y garantizar la integridad de los mismos. Como se puede ver en la figura 4.13, el procedimiento de envío definido protege completamente la trama MAC. Por un lado se firma la trama completa y se cifran los datos; empleando una función de resumen SHA-256 se obtiene la marca única de la trama entera, para posteriormente empleando la clave de sesión o la de difusión cifrar el resumen generado y los datos empleando AES. La cabecera MAC no se cifra dado que de otra manera no se podría determinar ni el origen ni el destinatario.

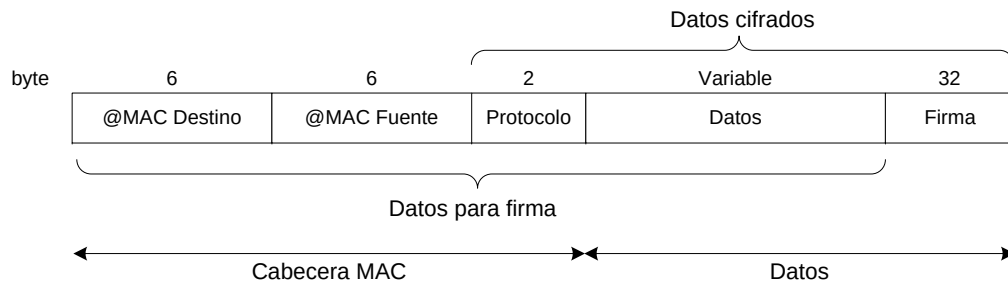


Figura 4.13: Formato de paquete cifrado y firmado entre nodos personales

Los algoritmos de cifrado de bloque, como es el caso de AES, requieren que los datos sean un múltiplo del tamaño de bloque, por lo que si los datos en claro no lo son se necesita añadir información de relleno. Este hecho repercute directamente sobre la unidad máxima de transmisión (MTU, *Maximum Transmission Unit*). Considerando una MTU de 1500 *bytes* y que el tamaño de la firma es de 32 *bytes*, restan 1468 *bytes* como máximo para la carga útil. Aplicando la condición de que los datos a cifrar deben ser múltiplo del tamaño de bloque del algoritmo (16 *bytes* para el caso de AES), se obtiene que la MTU de la UCL en el caso de incorporar todas las medidas para implementar un canal seguro a nivel de enlace es de 1456 *bytes*. La eliminación de este relleno en recepción será a cargo de las capas superiores, pues se considera que dichos protocolos incorporan un campo de longitud de mensaje o bien unas estructuras de datos fijas que descarten el relleno.

Aunque en la PN se apuesta por la seguridad extremo a extremo, en el nivel de enlace se aplica salto a salto, es decir, una ruta a través de nodos personales supone que cada intermediario descifra, redirige y vuelve a cifrar cada trama empleando para ello las claves correspondientes a los nodos anterior y posterior de la ruta. Los nodos personales son confiables y aunque inspeccionen información de los paquetes para determinar la ruta óptima no se considera un riesgo de seguridad. Es más, en caso de considerarlo, se podrían aplicar soluciones de seguridad a nivel de red y superiores. En la figura 4.14, el nodo B actúa como repetidor para las comunicaciones entre A y C. En este escenario el nodo A cifra la trama empleando la clave de sesión compartida con el nodo B, quien la redirige al nodo C empleando la clave compartida en este caso entre el nodo B y el C. Un nodo B' que quisiera inspeccionar los datos no podría, ya que las claves empleadas no son conocidas por él. Por tanto, la comunicación en modo multisalto está siempre protegida.

El modelo descrito se puede utilizar sobre cualquier nivel de enlace adaptando las características a las particularidades de cada uno. La idea subyacente siempre ha sido la de facilitar al usuario el manejo y gestión de la seguridad, incidiendo en la automatización de

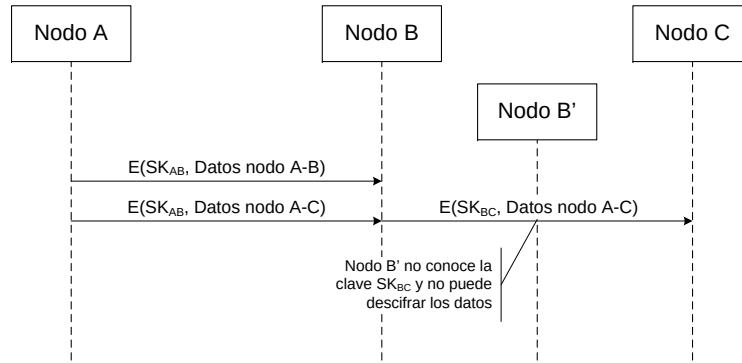


Figura 4.14: Seguridad a nivel de enlace en un escenario multisalto

los procesos. No obstante, algunas interfaces radio ya incorporan mecanismos de generación de sesión de claves temporales, como por ejemplo las tecnologías IEEE 802.11 usando WPA. En esos casos, se pueden aplicar los sistemas estándar tomando como clave raíz la clave bilateral de nivel de enlace, inyectándola directamente sobre la tarjeta de comunicaciones sin que el usuario tenga que realizar ninguna configuración. La misma solución podría aplicarse para el caso de tener que emplear PIN, etc.

4.5.2. Seguridad a nivel de red

Los mecanismos planteados permiten garantizar los intercambios entre nodos personales a nivel de enlace. Tomando la condición de personal como métrica para definir las rutas, se puede considerar que los intercambios extremo a extremo también son seguros. Sin embargo, en ocasiones resulta necesario emplear nodos externos con los que se carece de confianza para alcanzar el objetivo final. La seguridad a nivel de enlace no es suficiente y se deben definir procedimientos equivalentes pero a nivel de red.

A medida que se asciende en la pila de protocolos las soluciones de comunicaciones se hacen más abstractas y genéricas, es decir, las múltiples capas subyacentes comparten todo lo que se defina por encima de ellas. En la PN, además la UCL se define como nexo de unión ocultando la diversidad que exista por encima y/o por debajo de ella, y lo mismo se aplica a la seguridad. De forma global se emplea el protocolo IP como estándar *de facto*, para el que se han definido diversas soluciones donde la más usada es IPSec [167, 168]. IPSec consta de dos protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6: *Authentication Header* (AH) proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados y *Encapsulating Security Payload* (ESP) aporta confidencialidad y la opción de autenticación y protección de integridad. Dependiendo de los requerimientos de sistema y de la situación en particular se emplea uno u otro.

Internet Key Exchange (IKEv2) [169] es un conjunto de protocolos diseñado para crear un entorno protegido de comunicaciones que incluye la autenticación de los extremos y definir y gestionar la asociación segura entre nodos autenticados. IKEv2 es la base del protocolo IPSec y emplea un intercambio secreto de claves de tipo DH para establecer el secreto compartido y, a partir de ahí, cifrar la comunicación. Se definen dos fases. En una primera,

los extremos se dan a conocer, se autentican, acuerdan un secreto común gracias al cual cifran la negociación de los parámetros que definirán los intercambios seguros posteriores. Establecido el contrato entre los extremos, la segunda fase genera las claves temporales para las sesiones IPSec.

Dado que la K_{PN} se ha obtenido siguiendo un método robusto, se puede emplear IKEv2 con autenticación basado en claves compartidas tomando la clave personal como referencia. Para no comprometer la K_{PN} , siguiendo la estructura de claves multinivel, se define la Clave Maestra de Comunicaciones (CMCo) como la clave bilateral derivada de la K_{PN} que securiza el nivel de red para una dupla de direcciones personales y protocolo específico. Desde este punto se sigue el procedimiento estándar con el resto de la negociación IKEv2 y la operativa de canal seguro IPSec.

En cierto modo, el protocolo IKEv2 presenta numerosas similitudes con los procedimientos de seguridad definidos dentro de la PN. Tanto es así, que obviando la negociación de parámetros y presuponiendo un funcionamiento homogéneo en todos los nodos personales, se podría en cierto modo reemplazar la primera etapa de IKEv2 por el CPFP, quizás extendiendo de alguna manera la operativa de este último. Sin embargo, esta alternativa supondría la modificación del protocolo IKEv2 estándar, lo que no se plantea como aceptable por las consecuencias que acarrea sobre los nodos, principalmente falta de compatibilidad.

IPSec establece dos modos básicos de operación: modo transporte, donde sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada, y modo túnel, donde todo el paquete IP (datos más cabeceras) es cifrado o autenticado encapsulándolo en un nuevo paquete. El primero se utiliza para comunicaciones directas entre equipos usualmente dentro de la misma red, mientras que el segundo se utiliza para comunicaciones red a red (túneles seguros entre *routers*, redes privadas virtuales (VPN, *Virtual Private Network*), etc.) o comunicaciones entre iguales sobre Internet.

A la vista de lo anterior, se puede afirmar que IPSec se ajusta a la arquitectura definida dentro de la Capa de Abstracción a Nivel de Red. Dentro de los *clusters*, el encaminamiento multisalto ad-hoc obliga a conocer la dirección destino para poder determinar la ruta óptima para llegar a él. Emplear el modo túnel ocultaría esta información y, dado que el paquete original se encapsula en otro nuevo, en cada salto habría que desencapsularlo para analizar datos y cabeceras. Este modo de funcionamiento se asemeja al planteado anteriormente a nivel de enlace por lo que no supondría ninguna ventaja, ya que los nodos intermedios serían capaces de acceder a toda la información de nivel de red. Por el contrario, teniendo en cuenta que a nivel de enlace se cifra y autentica todo el paquete, y que existe la necesidad de, en cada salto, conocer el destinatario, el modo transporte sí ofrece mejoras en términos seguridad. Al descifrar la trama a nivel de enlace, toda la información de nivel de red queda en claro, pudiendo los nodos intermedios no sólo analizar las cabeceras necesarias para determinar el siguiente salto, sino también todos los datos que se transmiten si lo desearan. Con el empleo del modo transporte la carga útil del paquete IP quedaría oculta en cada salto, logrando así desligarla de la toma de decisiones de encaminamiento.

Como alternativa no restringida al nivel de red, sino basada en cualquiera de los protocolos que operan en la capa de transporte o por encima, se encuentra TLS [170, 171]. TLS es el sucesor natural de SSL y normalmente se emplea para encapsular protocolos de aplicación tales como *Hypertext Transfer Protocol* (HTTP), *Simple Mail Transfer Protocol*

(SMTP), etc. Aunque históricamente se implementa sobre TCP, existen versiones que operan en entornos UDP o *Datagram Congestion Control Protocol* (DCCP) usando *Datagram Transport Layer Security* (DTLS). Uno de los usos que se da a TLS es el de tunelizar una red completa y crear VPN, lo que de forma natural permite la extensión a la PN.

TLS sigue un modelo de negociación de claves de sesión basado en criptografía, aunque como en el caso de IPsec existe una alternativa para trabajar con claves pre-establecidas *Transport Layer Security Pre-Shared Key* (TLS-PSK) [172, 173]. Esta operativa es similar a la planteada anteriormente para IPsec, donde la clave compartida sería K_{PN} , con la salvedad de que en lugar de operar estrictamente a nivel de red, la solución encapsularía los paquetes en niveles superiores.

Independientemente de la opción que se emplee, para las comunicaciones inter-*cluster* es el modo túnel el que ofrece mayores ventajas. Dado que este tipo de comunicaciones se sustenta en la infraestructura de terceros, es importante ocultar toda la información personal a los nodos externos. Los nodos pasarela de cada *cluster* además de la dirección personal disponen de otra global dentro de la red sobre la que operan para proporcionar el acceso remoto. La operativa en modo túnel supone en este caso que todo el paquete IP personal se encapsula sobre el nuevo paquete IP que se transmite entre las direcciones públicas de los nodos pasarela. Los *routers* de la red podrán redirigir el paquete hacia el destino, pero siempre sin conocer la información personal que viaja en ellos. La dirección pública de los nodos pasarela es algo ya conocido y aunque proporciona información de la localización del *cluster*, es un riesgo que no se puede evitar y se tiene que asumir dentro de la PN.

En definitiva, la solución de seguridad a nivel de red planteada dentro de la PN emplea un protocolo estándar como es IPsec con IKEv2, con un proceso de autoconfiguración basado en el resultado del CPFP. Dependiendo del ámbito de aplicación, comunicaciones intra-*cluster* o inter-*cluster*, se opta por uno u otro de los modos de funcionamiento de IPsec. Dentro del *cluster*, y siempre que las rutas únicamente incluyan nodos personales, la robustez de la PN está suficientemente garantizada empleando sólo seguridad de nivel de enlace. No obstante el aplicar IPsec en modo transporte, una vez negociada la sesión, no incurre en mucha latencia extra dado que las operaciones de cifrado a nivel de red se realizan exclusivamente en los extremos y comparativamente la propia operativa multisalto ad-hoc incurre en un mayor retardo y degradación del rendimiento [174, 175].

4.5.3. Seguridad a nivel de servicio

La gestión de servicios dentro de la PN se realiza en 5 niveles tal como se reflejó en la figura 3.24 del apartado 3.6. Esta propuesta se basa en la existencia de un nodo denominado SMN que guía las tareas de publicación, descubrimiento y provisión de los servicios, siguiendo una estructura jerárquica hasta el nivel de *cluster* y colaborativa dentro de la PN.

El reto de la Capa de Abstracción a Nivel de Servicio es crear un entorno donde las transacciones puedan ser llevadas a cabo de una forma segura extremo a extremo. A pesar de que la solución de seguridad a nivel de red ya aporta esta experiencia, la seguridad se limita a nivel de dispositivo y mensaje sin considerar ni el contenido ni quién ha demandado

la información, es decir, el usuario. Los requerimientos a nivel de servicio ante todo se centran en habilitar un entorno autenticado de registro, búsqueda y uso de las aplicaciones o servicios, al tiempo que se garantice la integridad y confidencialidad de los datos. Ahora bien, esto no es suficiente. Los procesos definidos a nivel de servicio no se deben proporcionar por igual a todos. A nivel de red y de enlace todos los dispositivos personales tienen los mismos permisos, pero a nivel de servicio dependiendo del tipo de dispositivo, del contexto del usuario, del propio usuario y del servicio específico se delimitan diferentes niveles de acceso. Dicho de otra manera, se tienen que definir soluciones que provean de autorización. El GIAAC, empleando perfiles de seguridad, determina los permisos de acceso para un servicio en función de las credenciales del usuario. Estos perfiles describen los requerimientos y el nivel de confianza a cumplir. Se recomienda que la especificación de los perfiles siga procedimientos basados en ontologías y representación XML por la facilidad que ofrecen a la hora de poder evaluar y contrastar las políticas de acceso sobre ellos.

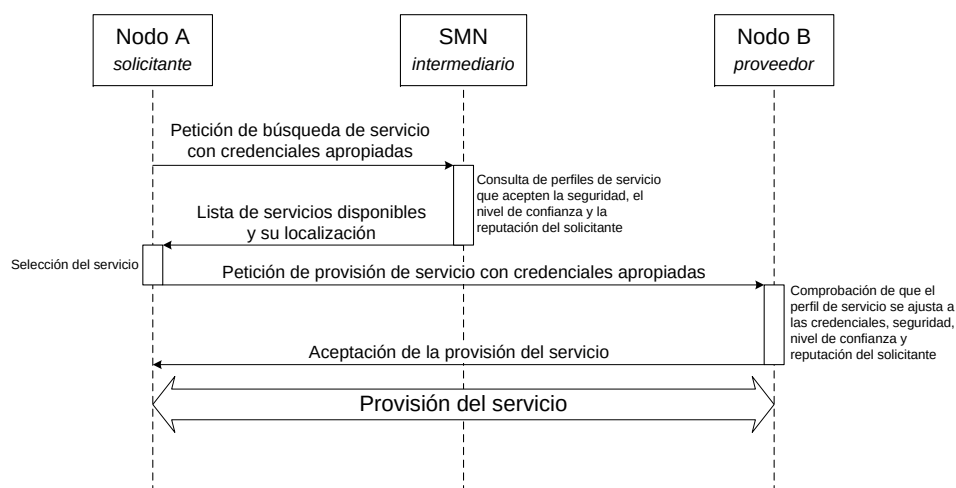


Figura 4.15: Provisión de servicio personal a un nodo personal

En las figuras 4.15 y 4.16 se muestra el procedimiento seguido para proveer un servicio. La primera describe el proceso de petición y provisión de un servicio entre nodos personales. El SMN se hace cargo de dirigir todo el proceso. Antes de retornar el listado de servicios disponibles con las características demandadas, analiza el perfil del nodo demandante para restringir los resultados únicamente a aquellos servicios que pueden entrar dentro de su nivel de autorización. Como resultado del descubrimiento el nodo personal dispondrá de las localizaciones de los servicios para el acceso directo a ellos, pero el SMN no puede conocer si tendrá o no permiso. Las respuestas del SMN se restringen únicamente al listado, mientras que la provisión del servicio es responsabilidad del nodo remoto. Será este nodo quien, en función del perfil adjunto a la petición de provisión y su carga de trabajo, acepte o no la solicitud.

Por su parte, la relación con los nodos externos es algo más compleja. El nodo externo tendrá acceso a la PN a través de un nodo personal que hará de intermediario y redirigirá la petición al SMN primero y posteriormente al nodo proveedor. La respuesta del SMN no incluirá la localización de los servicios, siendo el nodo intermediario quien, en función del identificador del servicio, reenvíe los mensajes. El perfil del servicio debe incluir la

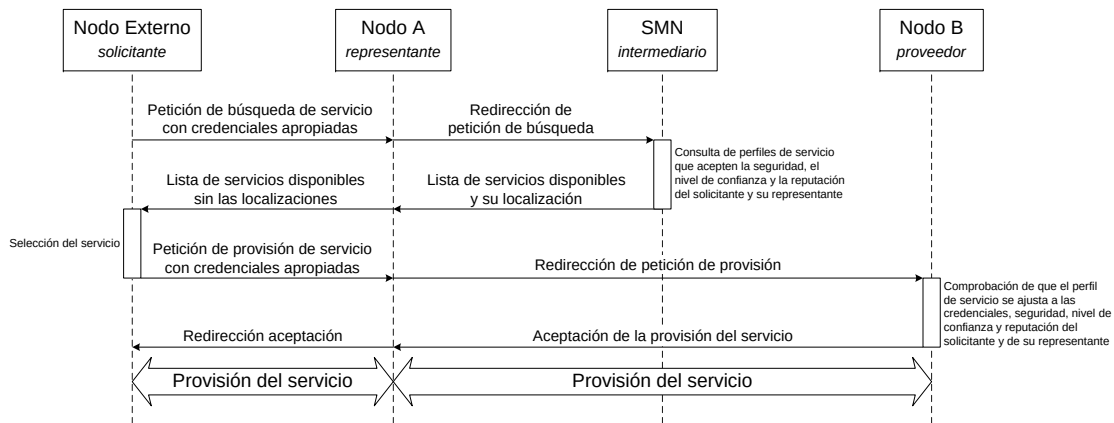


Figura 4.16: Provisión de servicio personal a un nodo externo

disponibilidad de un servicio para los nodos externos y las condiciones que debe cumplir tanto el propio nodo externo como el intermediario.

Adicionalmente los procesos de búsqueda de servicios del SMN pueden desembocar en el descubrimiento de servicios provistos por nodos externos. En caso de que este tipo de servicios sean proporcionados entre la lista de resultados en la respuesta del SMN, el usuario debe ser claramente notificado de ello, al tiempo que se le indicarán los requerimientos que tiene que cumplir para acceder al servicio. Es en estos casos donde el usuario, como último responsable, debe prestar especial atención y saber dónde y a qué accede para evitar el uso de servicios que puedan poner en riesgo la integridad de su PN.

Dentro del nivel global de búsqueda y provisión de servicios, definido como el nivel 5 de la arquitectura multinivel de servicio, no sólo nos podemos encontrar servicios provistos puntualmente por un único nodo externo, sino que éstos pueden estar asociados a proveedores o a otros usuarios. En estos casos, la implantación de modelos de confianza basados en reputación ayudarán al usuario de la PN a diferenciar qué servicios son más adecuados por estar mejor valorados. El esquema de reputación incluirá también la confianza que aporte la ruta de descubrimiento y provisión, es decir, la valoración de aquellos SMN y nodos que participen en las tareas. Ponderando la confianza en los nodos y la de éstos en el servicio que describen se obtiene el resultado final que se notifica al usuario [176].

A nivel de servicio, la necesidad de identificar al usuario se hace más patente. Algunas opciones pasan por poder discernir entre diferentes identidades virtuales o pseudónimos, confiar parte de esa identificación en el nodo que se supone personal, etc. Para identificar empleando el mismo identificador de usuario independientemente del servicio al que se acceda se pueden usar protocolos como *Open Authentication* (OAuth) [177, 178], donde se asocia un usuario y sus credenciales con unos permisos sobre diferentes aplicaciones. Para incrementar la seguridad en la identificación se están implantando los métodos basados en autenticación en dos pasos empleando contraseñas de un solo uso basadas en tiempo (TOTP, *Time-based One Time Password*). Estos últimos implementan la identificación en dos factores, lo que se tiene y lo que se sabe. Extenderlo e incluir un tercer factor, lo que se es, sería algo directo vinculando la generación de la clave a cualquier metodología de adquisición de información biométrica.

A diferencia del nivel de red donde prácticamente sólo se emplea una solución de comunicaciones, IP, y por tanto asegurarla es más sencillo, a nivel de servicio la diversidad de protocolos, métodos de acceso, etc. es muy elevada, lo que hace prácticamente imposible diseñar una única solución. Partiendo desde el nivel de transporte, donde el camino de forma genérica se bifurca entre TCP y UDP, ya se nota esa diversidad con soluciones como SSL, TLS, etc. A medida que se asciende de nivel, cada protocolo de aplicación incorpora sus propios mecanismos de cifrado. En todos ellos se puede emplear la K_{PN} como base de la negociación de claves, si bien su empleo únicamente autentica los dispositivos que intervienen en la comunicación.

4.5.4. Visión global

Una visión global de la aplicación de las soluciones de seguridad planteadas y su aplicación en los diferentes niveles se incluye el diagrama figura 4.17.

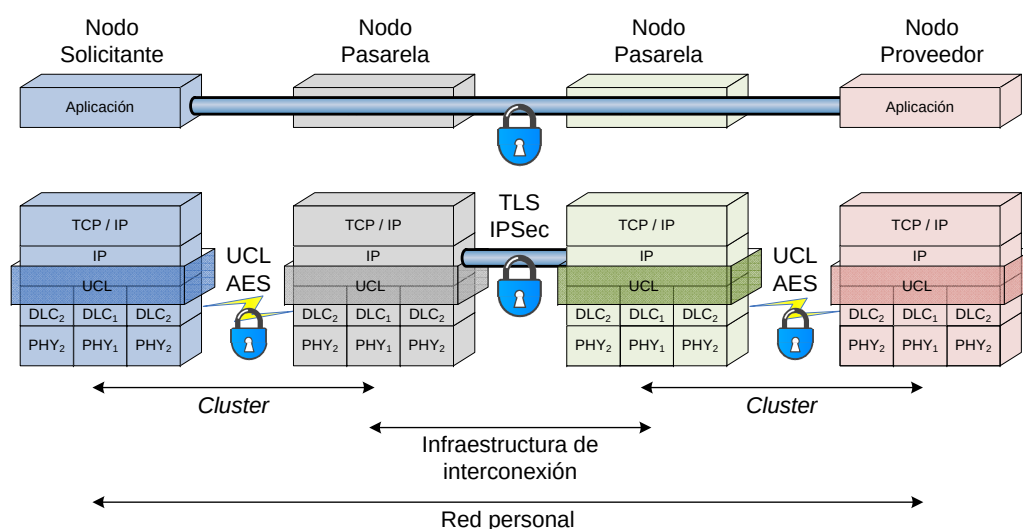


Figura 4.17: Visión global de la seguridad en una PN

La descripción realizada en este capítulo presenta una arquitectura de seguridad que cumple con los requisitos planteados para la PN, dotando de autenticación, integridad y confidencialidad a las comunicaciones que se realizan dentro de cualquier PN.

Partiendo del PFP y analizando sus virtudes y deficiencias se ha propuesto el CPFP como una versión mejorada que no sólo permite personalizar los nodos sino que aporta una solución integrada para la gestión de la pertenencia a la PN. Este sistema beneficia claramente al usuario, al que le facilita las tareas de control de su PN reduciendo y automatizando notablemente los intercambios a realizar entre sus nodos. Así se ha mostrado que de $O(n^2)$ operaciones, con el uso del CPFP se limitan a $O(n)$.

Del mismo modo que la arquitectura de la PN es una arquitectura multicapa, la seguridad sigue un esquema similar. Desde el nivel de conectividad al de servicio, pasando por el de red, se ofrecen propuestas que permiten extender las tradicionales soluciones de seguridad a un sistema tan peculiar como es la PN. Se ha puesto especial énfasis en solventar las

deficiencias y la heterogeneidad de soluciones de seguridad en la capa de enlace, donde el apoyo de la UCL es indispensable. Garantizar la integridad y confidencialidad en cada salto de forma eficiente permite además a los algoritmos de encaminamiento establecer rutas confiables y circunscribir todo el tráfico dentro de la PN.

Por otro lado, aunque la agrupación de PN ofrece a los usuarios un nuevo abanico de servicios no se deben olvidar los riesgos que esta apertura puede suponer. Dentro de la PN el usuario conoce y controla personalmente sus nodos y la gran mayoría de los accesos a sus servicios. Sin embargo, la colaboración con otros usuarios en la provisión de servicios supone que es necesario confirmar fehacientemente la identidad de éstos y establecer una relación de confianza limitada para el propósito de la colaboración. Estas restricciones reducirán el riesgo potencial de que la PN se vea afectada por usos malintencionados.

Capítulo 5

Federación de redes personales

Gran parte de lo que cada uno de nosotros es surge fruto de los vínculos que día a día establecemos unos con otros. Los seres humanos necesitan de estas relaciones para definirse como individuos y dar sentido a su existencia. Ya lo dijo Ortega y Gasset, «Yo soy yo y mi circunstancia»; todo lo que nos rodea nos afecta y nosotros nos proyectamos sobre nuestro entorno. De hecho, la manera de relacionarnos con los demás no es sino una extensión de la relación que tenemos con nosotros mismos y con todo lo nuestro. La única diferencia es que el entorno ya no se encuentra bajo nuestro control.

A diferencia de los animales, los seres humanos somos seres racionales, lo que nos dota con la capacidad de tomar decisiones. Las relaciones no son más que la materialización de algunas de esas decisiones y nos llevan a mantener esos vínculos más allá de la mera necesidad, incluyendo motivos irracionales o la mera voluntad de compartir o intercambiar conceptos, ideas o incluso recursos. Toda relación se mantiene ya que existe un conocimiento mutuo de lo que cada uno aporta y opina del otro, lo que dota a dicha relación de confianza. No obstante, la subjetividad de una relación personal supone que sea posible modificarla a voluntad de los participantes o por la influencia que se ejerzan entre ellos.

La importancia de las relaciones personales queda plasmada en el auge que las redes sociales han tenido en los últimos años. Las tecnologías de la información han proporcionado los medios y las personas no han dudado en usarlos. Una red social es una comunidad creada por individuos interconectados bajo un factor común, bien sea la amistad, la familia, etc. Algunas redes sociales populares, como Facebook [179] y Tuenti [180] vinculadas a las amistades y al ocio, LinkedIn [181] relacionada con la vida laboral u otras muchas existentes (Twitter [182], etc.), forman parte de nuestra vida cotidiana y han modificado la forma en la que mantenemos contacto con otras personas. Basadas por el momento en el envío de mensajes y la compartición de recursos multimedia, en algún momento darán un paso adelante y añadirán a su catálogo otras opciones como compartición de recursos físicos o lógicos.

En los capítulos anteriores se introdujo el concepto de PN como una red segura en el entorno del usuario que se auto-configura y auto-gestiona. Dada la importancia que, como se ha descrito, tienen las relaciones para los usuarios de esas PN, ¿por qué no extender el concepto de PN más allá de un único usuario? La respuesta a esta pregunta tiene nombre y apellidos y se denomina PN-F. La PN-F aspira a proporcionar funcionalidades similares

a las de una PN, pero extendiéndolas a grupos de usuarios con diferentes requerimientos y necesidades.

Una PN-F tiene que trasladar los fundamentos de las relaciones entre personas a elementos de red que permitan establecer relaciones entre dispositivos y, por ende, entre las personas que los poseen. Del mismo modo que una PN hace frente a la heterogeneidad, la amigabilidad, la seguridad o la confianza, una PN-F debe desplegar las soluciones técnicas que den las mismas garantías de uso.

De forma básica se puede concebir una PN-F como una red colaborativa, donde dispositivos diversos de múltiples usuarios cooperan para lograr un objetivo común. No obstante, dependiendo de la situación cada usuario ofrecerá, previo acuerdo, únicamente un conjunto de sus recursos manteniendo el resto a buen recaudo. Por tanto, una federación, además de generarse de forma automática y espontánea, independientemente de la localización de las personas participantes, debe heredar la confianza y la seguridad de la PN abriendo puertas únicamente a aquellas entidades colaboradoras.

Existen soluciones como las redes privadas virtuales o las redes formadas por aplicaciones P2P que dan una respuesta incompleta a las necesidades planteadas, pues no proporcionan ni la auto-configuración y ni la auto-gestión, e incluso carecen de la noción de grupo de confianza, centrándose normalmente en dar acceso a una red o aplicación específica. A esto se añade el hecho de que tampoco tienen en cuenta ni el contexto del proveedor del servicio ni de los potenciales clientes con los que se comparten los recursos. En este sentido, las soluciones actuales consideran las asociaciones de nodos de usuarios como algo estático con unas condiciones preestablecidas, muy lejos de lo que debería ser una PN-F, es decir, algo dinámico como la PN del usuario, donde se negocien tanto los recursos y servicios a compartir como el objetivo de la asociación y las condiciones de seguridad para formar parte de la federación.

Como se puede comprobar, la PN-F es un concepto muy extenso y presenta numerosos desafíos, entre los que se incluyen la especificación de metodologías para la definición, configuración y gestión de las federaciones, procedimientos para el descubrimiento y uso de servicios, tratamiento del contexto de los usuarios y de las propias federaciones, todo ello sin olvidar la seguridad. Partiendo de las ideas planteadas en [183], en este capítulo se ilustra el concepto de PN-F, resultado de la colaboración en el marco del proyecto MAGNET Beyond [25] y extendido con el trabajo en esta tesis. Considerando los retos y requerimientos de las PN-F se plantea la arquitectura y operativa de una PN-F, llevando a cabo los cambios necesarios sobre las PN existentes para hacer realidad la asociación de múltiples PN.

5.1. Concepto de federación

La PN se centra en la comunicación entre los dispositivos y nodos personales de un usuario en particular, y aunque de forma genérica considera la interacción de éstos con nodos externos, no contempla numerosos patrones que suponen extender la comunicación más allá de los límites de la PN con el propósito de colaborar con otras PN. Una PN-F puede definirse como una colaboración segura entre varias PN, de forma que un subconjunto

en modo ad-hoc, con las implicaciones que ello conlleva en cuanto a las soluciones que se implementen para desarrollar el concepto de PN-F. Este segundo tipo de federaciones usualmente tienen lugar entre las P-PAN de varios usuarios cercanos. Las PN-F híbridas, resultado de la combinación de los dos tipos anteriores, son también posibles.

Las PN-F se pueden clasificar considerando otras muchas características. Dependiendo de la forma en la que se origina e inicia una PN-F, se puede distinguir entre PN-F oportunistas o generadas bajo demanda. Las primeras se crean de manera espontánea cuando las circunstancias y el interés de los potenciales participantes confluyen, mientras que las segundas son el resultado de decisiones meditadas y su formación requiere de un ofrecimiento y petición explícita de un recurso. En ambos casos, aunque de manera más notable para el caso de las PN-F oportunistas, la información de contexto juega un papel importante. Otra forma de catalogar las PN-F según cómo se lleva a cabo el proceso de federación es usando los términos proactivos y reactivos, denominaciones que en cierto modo coinciden con los conceptos de oportunismo y bajo demanda.

Otra alternativa consiste en agrupar las PN-F considerando el tiempo de vida o duración de una PN-F, lo que hace que las soluciones a aplicar a la hora de establecer la federación también varíen. En federaciones cuya vida útil sea bastante efímera, no tiene sentido que los procedimientos de establecimiento y gestión sean complejos, por lo que se simplifican para no comprometer la creación de la federación. Este tipo de PN-F suele coincidir con aquellas que se generan de manera espontánea para dar respuesta a una necesidad puntual. Por el contrario, cuando se espera que la PN-F sea de larga duración, el proceso considera muchos más aspectos y la negociación de los términos de la federación se complican incluyendo mecanismos de gestión más completos.

Los tipos de PN-F enumerados agrupan las situaciones más usuales que involucran a varios usuarios con intereses comunes y cuyas PN son, por tanto, candidatas a formar una PN-F. Algunos ejemplos de escenarios proclives a desencadenar una PN-F son:

- Trabajo empresarial colaborativo, reuniones virtuales, conferencias, etc.
- Compartición de recursos en el ámbito privado o profesional.
- Redes sociales entre familiares o amigos.
- Redes virtuales para clases o aprendizaje a distancia.
- Redes inter-vehículos para apoyar la actualización de información de tráfico, estado de las vías, etc.
- Emergencias.

De forma análoga a la PN, en todos estos casos, los requerimientos principales para conformar una PN-F son que la red se auto-configure y auto-gestione manteniendo una comunicación segura entre los dispositivos que la conforman, todo ello teniendo en cuenta el contexto que rodea a los usuarios y sus dispositivos. No obstante, en el caso de la PN-F, la gestión de los miembros necesita de procedimientos adicionales, ya que no todo depende de un único usuario. La PN-F debe estar dotada de mecanismos que habiliten la confianza

no sólo entre los usuarios miembros, sino también entre el subconjunto de recursos de éstos (dispositivos, servicios, etc.) que participen en ella.

En este sentido, toda PN-F tiene un creador que define cuáles son las reglas de participación, es decir, la descripción del propósito de la PN-F y el comportamiento esperado por cada uno de los miembros. El creador, un usuario y su PN, verifica también la identidad del resto de las potenciales PN miembro, decide si su participación se ajusta a las políticas previamente establecidas y administrará el ciclo de vida de la PN-F. Por tanto, se definen dos roles en una PN-F: el creador y el miembro o participante. La figura 5.2 presenta los diferentes roles que pueden encarnar los usuarios de una PN-F y las relaciones que existen entre ellos. Como se puede observar, una PN-F sólo puede tener un creador, el cual realiza las tareas de gestión, si bien tiene la opción de delegarlas a una tercera entidad de confianza.

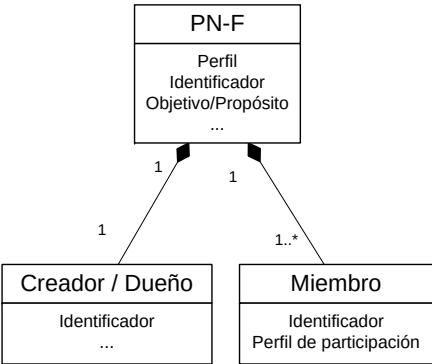


Figura 5.2: Relación entre roles dentro de una PN-F

A la vista de todo lo descrito, una PN-F es un concepto altamente ambicioso, que supone retos que van desde la definición del propio ciclo de vida y la especificación de las políticas de participación y uso, hasta el diseño de soluciones seguras para proporcionar la conectividad y la compartición de funcionalidades y servicios entre los nodos que la conforman. En el resto del capítulo se sentarán las bases de la PN-F considerándola como la extensión natural de una PN.

5.1.1. Terminología

Al igual que para la PN, en la tabla 5.1 se definen una serie de conceptos generales. Este conjunto de términos es el resultado de la adaptación de los especificados durante el trabajo en el proyecto MAGNET Beyond [135] al enfoque planteado en esta tesis.

Tabla 5.1: Terminología vinculada a la federación de redes personales

Federación de redes personales	Colaboración segura entre dos o más PN, que ponen a disposición un conjunto de servicios o recursos con el objetivo de alcanzar una meta común.
Miembro	Toda PN participante en una PN-F. Una misma PN puede ser miembro de varias PN-F como, por ejemplo, familia, trabajo, amigos, etc.

Tabla 5.1: Terminología vinculada a la federación de redes personales (continuación)

Invitado	Toda aquella PN que haya recibido una invitación para participar en una PN-F. El invitado puede no ser aún miembro de la PN-F.
Dueño o creador de la PN-F	PN miembro (o tercera parte) responsable de la concepción y creación de la PN-F así como de su destrucción. Por tanto, es el que en primera instancia controla el perfil de la PN-F.
Administrador	PN miembro (o tercera parte) con autorización para gestionar el perfil de la PN-F.
Perfil de la PN-F	Documento descriptivo de las características de una PN-F, donde se especifican las políticas y normas de uso. Adicionalmente puede incluir un listado de los miembros de la PN-F.
Perfil de participación	Para el caso de PN-F predefinidas, permite conocer el listado, descripción y políticas de uso (no tienen que ser idénticas para todos los miembros) de los servicios y recursos puestos a disposición de la PN-F por cada miembro. Se trata de un perfil específico para una PN-F. Para las PN-F espontáneas, en las que no existe un perfil predefinido, el perfil de participación incluye una descripción de los intereses del dueño de la PN y las políticas y reglas que deben cumplirse para la colaboración en nuevas federaciones. Se trata de un perfil genérico.
Directorio de redes personales	Tercera parte de confianza que, entre otras tareas, actúa como autoridad de certificación para autenticar a los miembros de una PN-F.
Listado de miembros	Lista de los participantes activos, almacenada en el perfil de la PN-F. Incluye a aquellos que se han unido satisfactoriamente a la PN-F y proporciona los detalles para el establecimiento del primer contacto con cada miembro. Adicionalmente este listado puede incorporar información de presencia, localización, etc.
Asistente de federación	Entidad funcional que gestiona la participación de una PN en una PN-F, así como los perfiles de PN-F y de participación resultantes. Puede encontrarse implementada de forma distribuida en los diferentes <i>clusters</i> o bien en la infraestructura de operador, como por ejemplo en el agente de la PN.

5.2. Ciclo de vida

A partir de la descripción de alto nivel del concepto de PN-F, se deduce que el proceso de federación define un ciclo de vida durante el cual el comportamiento de las PN se adecua a las necesidades que impuestas por la PN-F. La figura 5.3 describe este ciclo de vida derivado de los retos y conceptos planteados y que define cinco grandes etapas: 1) definición, donde el creador de la PN-F establece el objeto de la PN-F y las reglas de participación, formación y uso, 2) participación, donde los potenciales miembros y el creador negocian los parámetros para adherirse a la PN-F, 3) formación, donde se establecen los medios de comunicación dentro de la PN-F asociando de manera segura las PN participantes, 4) uso u operación, donde se materializa la compartición de recursos de la PN-F, y 5) disolución o escisión de la PN-F, momento a partir del cual el creador o alguno de los miembros deja de compartir sus recursos.

A continuación se profundiza en cada una de estas etapas y su desarrollo según el tipo de PN-F. Las diferentes fases involucran la interacción de componentes de alto nivel, entidades y relaciones que se materializarán en el momento de definir la arquitectura específica de la PN-F en el apartado 5.3.

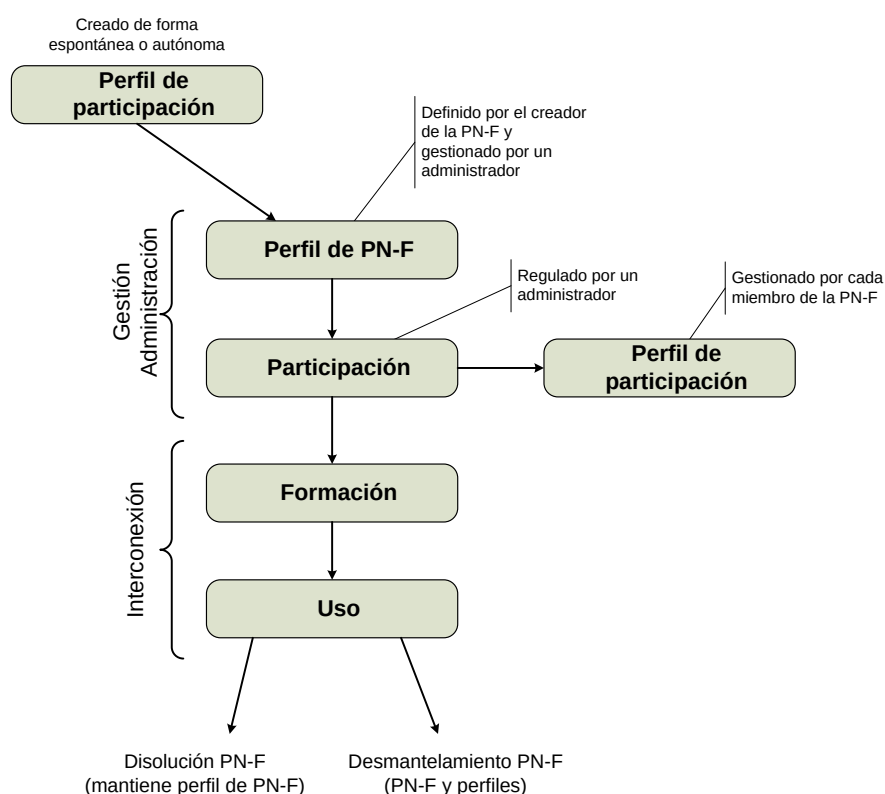


Figura 5.3: Ciclo de vida de una PN-F

5.2.1. Definición de perfiles

Para poder establecer relaciones seguras y fructíferas entre PN se requiere definir una serie de reglas que definan el comportamiento de las PN y garanticen la confianza entre ellas. Enumerar qué PN son miembro de la PN-F o definir las condiciones para serlo, forma parte de lo que se denomina gestión de membresía. Por su parte, cada miembro dentro de la PN-F necesita definir qué recursos pone a disposición de ésta y en qué condiciones, lo que se denomina gestión de recursos.

Tomando como definición de perfil dentro de una PN-F el conjunto de descripciones, normas o políticas a través de las cuales se regula el comportamiento de la PN-F y relacionándolo con los dos ámbitos de gestión anteriores, se identifican dos perfiles: el propio perfil de la PN-F y el perfil de participación de cada PN miembro. En la figura 5.4 se muestra la relación entre ambos. Mientras que el perfil de la PN-F es único y común para todas las PN, el perfil de participación está ligado a cada miembro individualmente e incluye su visión particular de la PN-F.

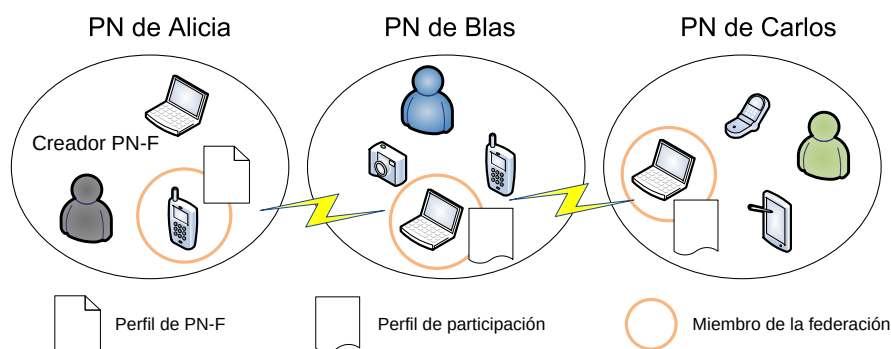


Figura 5.4: Perfiles dentro de la PN-F

5.2.1.1. Perfil de la PN-F

El perfil de la PN-F establece las condiciones de partida de ésta. Contiene las políticas, normas y acuerdos comunes a toda la PN-F, a los que todo miembro participante o que desee participar debe adherirse.

Para que una PN-F pueda existir alguien debe haberla definido, por lo que, como se ha insistido, toda PN-F tiene un creador. Es éste quien administra el perfil de la PN-F. El papel de creador puede ejercerlo uno o más usuarios de PN y no necesariamente tiene que pasar a ser miembro de la federación. De esta forma se facilita la delegación de responsabilidades de administración en terceros. Adicionalmente, el creador o dueño de la PN-F puede definir una lista de administradores o usuarios con privilegios especiales con los que compartir las tareas de gestión de la PN-F, esto es, modificar el perfil de la PN-F y evaluar su correcto cumplimiento.

La definición del perfil se puede realizar con antelación en previsión de un uso o de forma instantánea en el momento que dos o más PN observan esa necesidad. Parte de la información incluida en el perfil son las reglas de acceso. En este sentido, el perfil de la PN-F, además de poder incluir períodos limitados de disponibilidad de la PN-F, puede

incluir explícitamente los miembros, referenciados por su identificador de PN, sin menoscabo de aceptar nuevos miembros siempre que cumplan con las condiciones establecidas. Los nuevos miembros pasan a serlo bien por invitación o porque ellos lo solicitan, en cuyo caso se requiere la aprobación del creador, de uno de los miembros, de la mayoría de los miembros o de todos según se fije en el perfil. No obstante, todos estos procesos se pueden automatizar si así se refleja en el perfil de la PN-F, de forma que la concordancia entre las políticas de la PN-F y las características particulares de los potenciales miembros se validan mediante motores de decisión sin necesidad de involucrar a los usuarios miembros.

El perfil de la PN-F es un documento vivo que se actualiza para dejar constancia de los nuevos miembros o de aquellos que han abandonado o han sido expulsados. En algunos casos se podrán modificar también las condiciones de uso, si bien no es recomendable ya que conllevaría no sólo propagar los cambios a todos los miembros, sino una renegociación total o parcial de los acuerdos de participación de cada miembro, lo que ocasionaría una degradación en la QoE. Por supuesto la modificación de la información contenida en el perfil se restringe al creador y a aquellos que haya designado como administradores.

Según lo expuesto, se puede resumir que el perfil de la PN-F debe como mínimo incluir:

- Características de la PN-F:
 - Nombre o identificador.
 - Objetivo o propósito.
 - Creador.
 - Lista actualizada de miembros.
 - Direcciones de contacto.
- Políticas de participación:
 - Lista fija de miembros.
 - Condiciones de aceptación/revocación de miembros (p. ej. por el creador o por consenso, etc.).
 - Políticas de privacidad.
- Otras normas, derechos, acuerdos:
 - Reglas de formación: duración temporal, eventos de activación, etc.
 - Aspectos legales que los miembros deben aceptar.

La información incluida en el perfil de la PN-F permite entre otras publicitar la PN-F. No obstante, todos los datos incluidos no se pueden considerar de carácter público. Será únicamente cuando una PN pase a ser miembro de pleno derecho cuando esa PN tenga acceso a toda la información. Se garantiza así la obligación de tener que establecer una relación de confianza y mantener un canal de comunicaciones seguro para conocer todos los detalles de la PN-F y compartir entre los miembros. La información privada del perfil, cifrada con claves propias de la PN-F, está formada, entre otras cosas, por el listado de

miembros más actual, manteniendo oculta y protegida la identidad las PN miembro y su rol dentro de la PN-F (administrador, etc.), por servicios o funcionalidades especiales, etc.

Si bien el perfil de la PN-F lo genera el creador de la PN-F, puede estar alojado en entidades de confianza en la infraestructura para facilitar su descubrimiento y accesibilidad. También existe la posibilidad de usar metodologías de almacenamiento distribuido, recomendadas en el caso de PN-F ad-hoc.

Para finalizar, se ilustra el concepto de perfil de PN-F con ejemplos de escenarios usuales. En una PN-F creada para su uso en el ámbito de una familia, el padre define los recursos y servicios del hogar que sus hijos pueden emplear. Este caso escenifica una PN-F generada por una entidad de confianza (el padre), que en principio no tiene por qué participar en la PN-F, definiendo un conjunto inicial de funcionalidades que posteriormente los participantes (los hijos) podrán extender con sus servicios particulares (teléfonos, juegos, etc.). En otro escenario, enfocado al trabajo colaborativo, el jefe de proyecto incluye por defecto a todos los trabajadores vinculados a ese proyecto, definiendo las condiciones para compartir los servicios y dispositivos que emplear durante la reunión semanal. Además, incluye la posibilidad de aceptar nuevos miembros, bajo su supervisión, por si compañeros de otros proyectos quieren unirse a la reunión. Estos son dos casos que se ajustan al formato de perfil de PN-F especificado a lo largo de esta sección.

5.2.1.2. Perfil de participación

Mientras que el perfil de la PN-F es común para toda la federación, cada miembro de la PN-F debe tener bajo su control los nodos, servicios, recursos y funcionalidades que aporta a la PN-F. A través del perfil de participación el usuario gestiona su PN dentro de la PN-F.

El perfil de participación es algo personal y privado que, en cierto modo, es un extracto del perfil de un usuario (preferencias, servicios, recursos físicos, etc.). El perfil de participación tiene que estar en sintonía con el perfil de la PN-F a la que va dirigido. Puede ser genérico o específico, es decir, creado y adaptado a la PN-F en la que se desee participar detallando los recursos que se comparten. En ambos casos el perfil incluye los intereses, fija los requisitos para crear o participar en nuevas PN-F y expone el conjunto mínimo de recursos que se compartirán.

La información mínima que debe estar disponible es:

- Dispositivos, recursos y servicios que un miembro quiere poner a disposición del resto de los miembros de la PN-F, incluyendo las políticas de acceso y el detalle de las normas de uso.
- Intereses personales del usuario para participar en una federación (información especialmente útil en federación de creación espontánea).
- Preferencias del usuario e información de seguridad.
- Acuerdo de aceptación de las normas de seguridad y condiciones de uso de la PN-F.

A diferencia del perfil de la PN-F, el perfil de participación puede sufrir modificaciones durante la fase de negociación para ajustar su contenido a las reglas y políticas de la PN-F.

Dependerá de la voluntad del usuario en participar en la PN-F el adaptar o no su perfil de participación.

5.2.2. Participación en la PN-F

Tras definir la información y reglas que guían la PN-F, llega el momento de establecer la comunicación segura entre los usuarios que desean compartir sus recursos. La etapa de participación supone la configuración del grupo de colaboradores, es decir, poner en contacto a los potenciales participantes y llevar a cabo las negociaciones para acordar las condiciones finales de uso de la PN-F.

Para que una PN se adhiera a una PN-F, el dueño de la PN-F debe publicitar su descripción de forma accesible para los potenciales miembros (p. ej. en un directorio conocido) o, proactivamente, notificar o invitar a otras PN. Debe tenerse especial precaución en no incurrir en difusiones masivas de invitaciones que puedan hacer considerar estos mensajes como *spam*. Podrán existir además invitaciones de PN-F fraudulentas, a lo que cada usuario, al tener control sobre su propia PN, podrá responder definiendo filtros que eliminen tráfico potencialmente peligroso o bien suscribiéndose a listas de PN-F maliciosas.

En cualquier momento, un usuario empleando las herramientas disponibles realizará la búsqueda de las PN-F que se ajusten a sus intereses. El análisis de coincidencias con las etiquetas y descripciones introducidas por el usuario se lleva a cabo sobre la parte pública del perfil de la PN-F. La información pública divulgada no debería incluir detalles de la PN-F más allá del propósito de la PN-F, los términos mínimos de operativa y la identidad del creador. Se recomienda que la parte pública del perfil de la PN-F incluya información que permita validar la identidad del creador, pues en la mayoría de los casos la confianza en él será decisiva a la hora de tomar la decisión de continuar con el proceso. El soporte de una TTP que certifique los datos del perfil resultará de gran ayuda tanto para federaciones apoyadas en la infraestructura como en ad-hoc.

Tras decidir a qué PN-F unirse, se ponen en marcha los diferentes procedimientos para añadir nuevos miembros a la PN-F. Una vez autenticado el creador de la PN-F y establecida una relación de confianza preliminar con él, la PN solicitante crea su perfil de participación particular para esa PN-F, el cual adaptará durante el proceso de negociación añadiendo o eliminando recursos, modificando las políticas de acceso, etc. según las directrices del perfil de la PN-F. Tras llegar a un acuerdo, el perfil común de la PN-F se actualizará para incluir al nuevo miembro y sus características.

Durante la vida de una PN-F, muchas serán las PN que se anexionarán o se separarán, lo que provocará la actualización del perfil. En cualquier momento, como respuesta a situaciones inesperadas, como por ejemplo la detección de ataques, por acuerdo global entre los miembros, se puede decidir reforzar ciertas políticas. En general, es recomendable que las características y políticas de la PN-F no estén fuertemente ligadas a la pertenencia o no de sus miembros, sino que éstos deben adaptarse a ellas. De esta forma, se evitará la renegociación segura de todos los parámetros cada vez que la lista de miembros se vea modificada. Sin embargo, es inevitable tener que generar y distribuir el conjunto de claves de seguridad que rijan la PN-F.

5.2.3. Formación de la PN-F

La siguiente etapa en la vida de una PN-F es la fase de formación. Toda vez que cada miembro haya ajustado su perfil de participación a las condiciones establecidas por el perfil de la PN-F, puede establecerse la federación, por lo menos a nivel de red, manteniendo comunicaciones seguras entre sus miembros. Como extensión de la PN, una PN-F opera y se mantiene a diferentes niveles de la arquitectura de red, por lo que el hecho de disponer de enlace de comunicaciones con algún nodo de otras PN de la misma PN-F no garantiza el acceso a todos los recursos ni servicios.

La solución que se adopte para implementar la PN-F será la que regule el establecimiento y negociación segura de los parámetros de conectividad y red. Dado que existen diferentes enfoques, los procedimientos no son únicos. Las particularidades de las diferentes arquitecturas planteadas en esta tesis para dar respuesta a la PN-F se describen más adelante en el apartado 5.3.

5.2.4. Uso de la PN-F

La fase de uso engloba el acceso seguro a los servicios y la provisión de éstos según las reglas acordadas en el perfil de la PN-F. La SMP y la SCMF asumen la responsabilidad dentro de la PN-F de garantizar el cumplimiento de las políticas de la PN-F y adaptar, en la medida de lo posible, el comportamiento de los servicios al usuario y su PN [135, 139].

Como se ha dicho, una PN-F se asemeja a una red social en su concepción. Así, la realimentación por parte de los usuarios que la conforman sobre los recursos y servicios disponibles aporta una estimación sobre la calidad real de la PN-F. En PN-F con un enfoque claramente público y global, estas valoraciones podrán incorporarse al perfil de la PN-F, lo que ayudará en la toma de decisiones durante la búsqueda de nuevas PN-F.

En este sentido, la SCMF, como gestor de la información de contexto y perfiles de usuario, proporciona los medios para adaptar la experiencia de uso al entorno y necesidades del usuario, haciendo la participación en una PN-F algo singular para cada PN.

5.2.5. Disolución de la PN-F

En cualquier momento un miembro de una PN-F puede decidir modificar su perfil de participación para dejar de compartir alguno de sus recursos. Esta situación supone que todas aquellas sesiones que involucren a cualquiera de esos recursos o servicios se darán por terminadas, teniendo además que notificarse al resto de los miembros de la PN-F la nueva situación para evitar que traten de acceder a ellos.

Llevar este escenario al límite supone que un miembro decide abandonar la PN-F, por ejemplo porque ésta no haya cumplido sus expectativas. En este caso, todos sus servicios y recursos dejan de estar disponibles en la PN-F pero, del mismo modo, todo aquello compartido en la PN-F deja de estar a su alcance. Como resultado de esta acción, es obligatoria la actualización y posterior difusión de un nuevo perfil de la PN-F, en el que se eliminará la PN del listado de miembros y se modificarán los parámetros de seguridad como claves de PN-F o de grupo, etc. Será alguno de los administradores de la PN-F o,

en su defecto, el creador quien lleve a cabo esta actualización, evitando así que el antiguo miembro tenga aún acceso a la PN-F.

Se puede dar también el caso en el que algún participante mantenga una actitud inapropiada, que implique un incumplimiento de los acuerdos negociados, es decir, de las políticas y reglas de la PN-F. El administrador se reserva el derecho de inhabilitar a dicho usuario y revocar la participación de su PN. Como en el caso anterior, se debe garantizar que la relación de confianza entre el resto de los miembros no se vea comprometida, actualizando el perfil de la PN-F pertinentemente.

Por último, por voluntad propia, el creador puede clausurar de forma temporal o permanente la PN-F. Se da la misma situación en el caso que el perfil de la PN-F defina períodos limitados de disponibilidad y/o operatividad. En caso de parada temporal, el mismo perfil podrá ser utilizado posteriormente, mientras que en el otro caso, la ausencia del responsable de la PN-F puede llevar al resto de los miembros a finalizar definitivamente su relación o, de forma espontánea, generar una nueva PN-F tomando como base las condiciones de la anterior. En la mayoría de los casos, estos escenarios se dan cuando el creador quiere delegar sus responsabilidades, con lo que el problema se solventa con la designación de un nuevo creador o el traspaso de las tareas, permisos y responsabilidades a cualquiera de los administradores. De esta manera se asegura la estabilidad de la PN-F y se evita tener que ejecutar nuevamente todo el proceso de creación y formación de la PN-F desde cero.

5.2.6. Otra perspectiva del ciclo de vida

En las secciones anteriores se ha analizado de forma global el concepto de PN-F y su ciclo de vida. La figura 5.5 resume la evolución en la relación entre el creador y los miembros de una PN-F. El diagrama profundiza en cada una de las etapas y representa la transición de estados desde el punto de vista del creador y de los miembros. Las etapas definidas en este diagrama se aplican tanto a la participación basada en invitación, como a la basada en la publicación del perfil.

5.3. Arquitectura

La definición del ciclo de vida ayuda a identificar las necesidades que plantea el despliegue de una PN-F. Aunque puedan existir ciertas similitudes con la formación de una PN, el hecho de hacer colaborar a varios usuarios supone el planteamiento de soluciones adicionales sobre las ya existentes en la PN, siempre sin olvidar características como la seguridad, la flexibilidad y la escalabilidad.

La PN-F plantea la colaboración a través de la compartición de recursos. La mayoría de las ocasiones la PN-F se define para explotar un servicio. Pero es erróneo centrarse únicamente en el nivel de servicio, pues los recursos de una PN no son sólo servicios, sino también los elementos de red, etc. De hecho, antes de compartir un servicio, primeramente tiene que existir una conexión segura entre las PN. En este sentido, es complicado identificar una única solución válida que cubra todos los posibles escenarios.

A partir del análisis de las diferentes etapas del ciclo de vida, se identifican un conjunto de funcionalidades genéricas que toda implementación de la PN-F debería incluir: seguridad

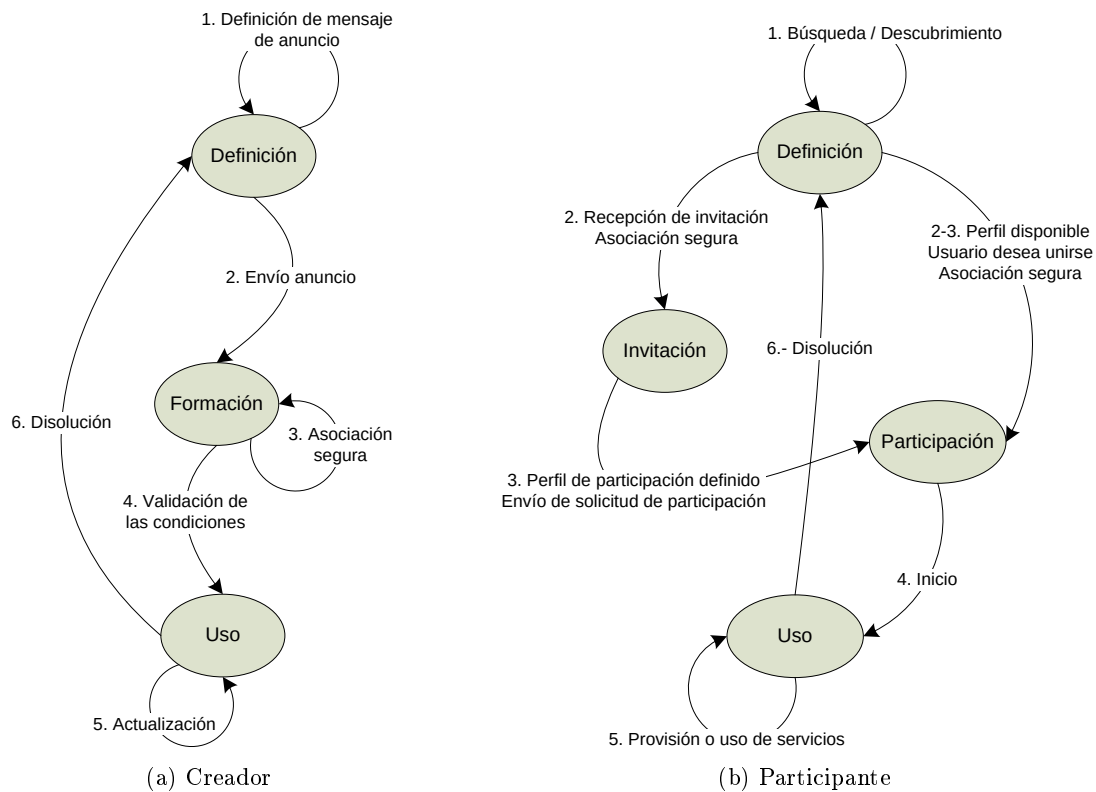


Figura 5.5: Diagrama de estados de los participantes en la PN-F

y confianza entre los miembros, gestión del intercambio de información entre PN y análisis de la correspondencia entre los perfiles de participación y el de la PN-F. El acceso final a los servicios compartidos, adaptándolos al contexto, requiere únicamente la extensión de las plataformas de servicio y contexto definidas en el ámbito de cada PN para que den respuesta a los requerimientos de la PN-F, por lo que no se considera la definición de nuevas entidades funcionales sino la adaptación de las ya existentes.

La PN-F es ante todo una red segura y debe garantizar el cumplimiento de su propósito por parte de sus miembros, lo que implica validar su identidad y sus perfiles, partiendo por los del creador. El uso de CPFP y el paradigma de PKI personal como mecanismos para dotar la confianza dentro de la PN permite extender la confianza a otras PN-F de una forma relativamente sencilla. Emplear una entidad de confianza superior que avale los certificados personales puede ser la solución. Se define el directorio de redes personales (PNDS, *Personal Network Directory Server*) como la entidad común a todas las PN-F que actúa como TTP emisora de los certificados personales de todas aquellas PN que deseen federarse. Tanto en los modos infraestructura como ad-hoc se verán beneficiados por la confianza que otorga esta entidad.

Pero de nada vale tener confianza entre PN si éstas no pueden interaccionar. Cualquier PN debe incorporar un punto de contacto que ejecute las tareas de gestión que impliquen la participación en una PN-F (autenticación y control de acceso, transferencia de perfiles de participación, etc.). El emplazamiento natural para esta funcionalidad, a la que se ha

denominado asistente de federación (FM, *Federation Manager*), son los nodos pasarela o *gateways* de cada PN.

Resta ya sólo definir cómo contrastar el cumplimiento de las políticas y reglas de la PN-F por parte de cada miembro. Con la intención de liberar de responsabilidades al FM, se define el evaluador de políticas (PE, *Policy Engine*) como el motor cognitivo que interpreta las expresiones semánticas incluidas en los perfiles de participación y las valida contra las políticas enumeradas en el perfil de la PN-F, aprobando o denegando el acceso y uso de los recursos de la PN-F.

Considerando estos elementos comunes a cualquier planteamiento que de una PN-F se haga, en la figura 5.6 se muestra la arquitectura genérica de una PN-F, asociando cada entidad funcional a su nivel de operación. Como se puede comprobar, el FM puede tener un mayor sentido operando desde nivel de red, mientras que las funcionalidades asignadas al PE se ejecutarían en niveles más altos.

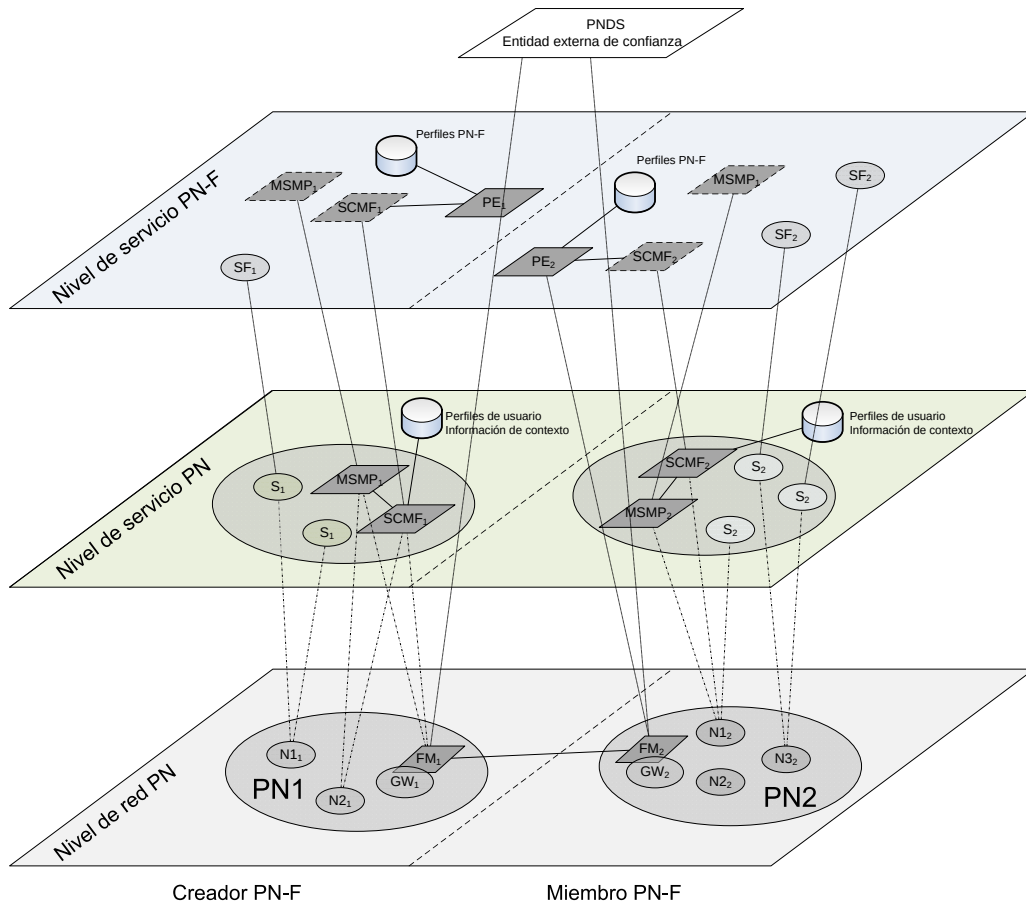


Figura 5.6: Arquitectura y entidades funcionales de una PN-F

Tomando como punto de partida la arquitectura genérica descrita en el contexto de esta tesis, aprovechando el marco del proyecto MAGNET Beyond, se han identificado diferentes formas de materializar una PN-F, cada una de ellas conduciendo al planteamiento de diferentes arquitecturas [139], de entre las que destacan especialmente tres. Centrada en

el nivel de servicio, la PN-F se puede constituir a través de un intermediario de servicio o mediante la extensión de la red superpuesta de servicios de la PN.

En el primero de los casos, reflejado en la figura 5.7a, toda la comunicación de la PN-F parece que se origina y termina en los propios nodos pasarela, dando la sensación de que los servicios se proveen y consumen desde ellos.

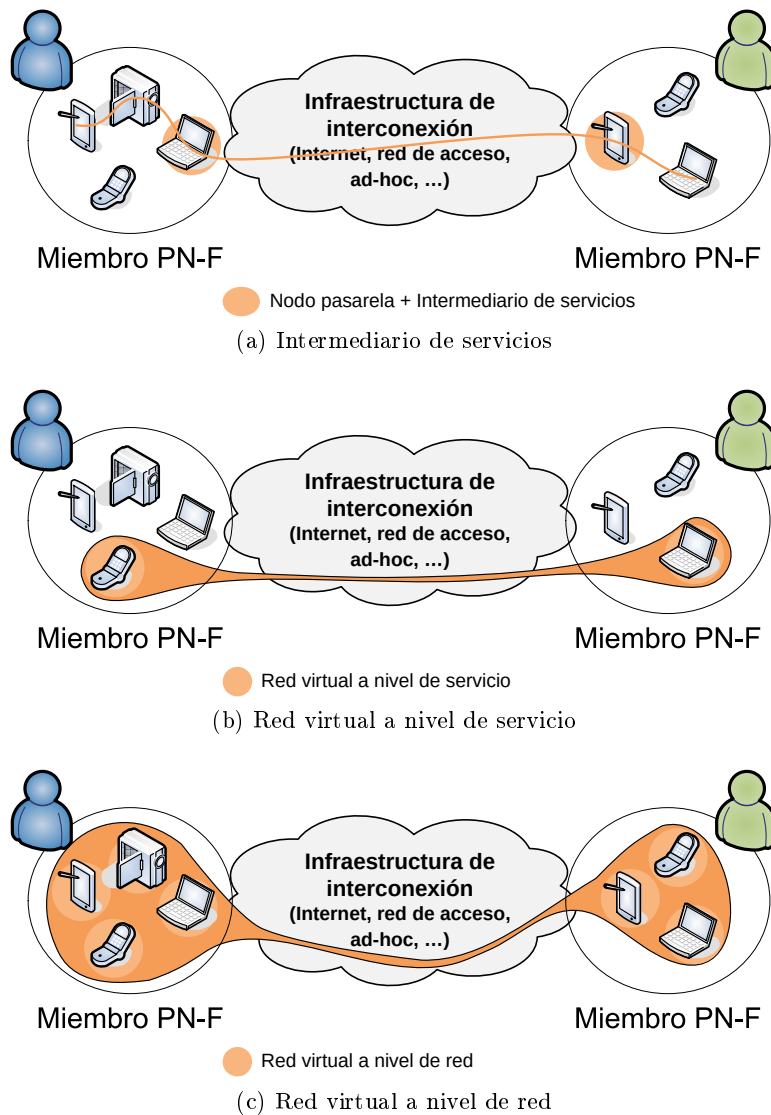


Figura 5.7: Arquitecturas de PN-F

La segunda alternativa, descrita en la figura 5.7b, extiende el paradigma aplicado en la SMP para el intercambio de información de servicios de los SMN. En esta ocasión, serán los nodos implicados en la PN-F los que intercambiarán la información de servicio, tanto descripciones, como de búsqueda y de provisión, generando una red a nivel de servicio que se apoya sobre la infraestructura de red existente. En este caso, sólo los nodos participantes son conscientes de la existencia de la PN-F. Sin embargo, lograr la comunicación segura de

larga distancia entre nodos de redes espontáneas multisalto resulta complicado empleando soluciones estándar de encaminamiento IP. Por tanto, se hace necesario adaptar los niveles inferiores para dotar de conectividad a los nodos.

La tercera opción, en contraposición con la anterior, considera todos los recursos de las PN a la hora de federarlas y, por tanto, permite ofrecer una solución similar en cuanto a filosofía, pero enfocada a nivel de red. Prolongando la arquitectura de una PN se establece una red virtual entre los dispositivos que forman parte de la PN-F, que servirá como medio para acceder a aquellos servicios que se compartan. La figura 5.7c resume la filosofía de esta alternativa.

Cualquiera de las tres arquitecturas es igual de válida aunque, como se ha citado, la segunda opción es la que plantea una mayor dificultad en su desarrollo. A continuación se describen las aproximaciones planteadas a nivel de red y de servicio, siendo la PN-F basada en una red virtual la que se detallará en mayor profundidad. Además, ésta es la opción que se ha implementado y validado [88, 184-186], pues plantea la PN-F como la extensión natural de todas las funcionalidades de la PN, es decir, establece primeramente un nivel de red seguro sobre el que posteriormente provisionar los servicios adaptados al contexto.

5.3.1. Entidades funcionales comunes

Seguidamente se describe la arquitectura de los componentes funcionales que se consideran comunes a cualquier implementación de la PN-F: el FM, el PNDS y el PE. Cada una de estas entidades funcionales no tiene que implementarse en un único nodo o dispositivo, sino que pueden ofrecerse de forma distribuida.

5.3.1.1. Directorio de redes personales

Para iniciar cualquier PN-F es necesario que se cumplan dos condiciones: identificar aquella PN-F que dé respuestas a los deseos de los potenciales participantes y garantizar que tanto el creador como los participantes son de confianza. El PNDS se define con el objetivo de atender esas necesidades, actuando como TTP y como directorio de perfiles de PN-F. El PNDS es una entidad autónoma, no dependiente de un usuario, cuya arquitectura de despliegue es responsabilidad del proveedor de la funcionalidad.

Dentro de cada PN, la PNCA garantiza la identidad de los diferentes dispositivos y nodos de una PN y, por extensión, es la base de la red segura que éstos conforman. La PNCA es validada por el propio usuario durante su creación. Sin embargo, este proceso no es suficiente cuando se trata de establecer la confianza con otras PN, a no ser que los diferentes usuarios se distribuyan de manera segura sus certificados personales. Este mecanismo no es en absoluto escalable y está sujeto en muchos casos a una posible suplantación de identidad.

El PNDS es la entidad encargada de proporcionar esa confianza al actuar como CA de nivel superior. En este sentido, la operativa de personalización de nodos en una PN debe modificarse ligeramente. Al iniciar la PNCA, su certificado personal (raíz de la seguridad en la PN) debe ser remitido al PNDS, quien firma y valida la identidad de la PN. Esto implica que la PNCA tendría que estar conectada a la infraestructura. A partir de ese momento, la PNCA operará como CA delegada.

La autenticación de la PN se puede hacer siguiendo los tediosos procedimientos naturales de una PKI [187] o bien definir algo más sencillo, usable y cercano al usuario. En este sentido, como se verá en el capítulo 6, en esta tesis se ha propuesto y desarrollado un procedimiento donde el PNDS autentica a los usuarios o PN empleando un algoritmo basado en un identificador de usuario vinculado a su terminal móvil y un conjunto de claves de usuario que desbloquean claves criptográficas de autenticación, las cuales se pueden vincular a diferentes perfiles de participación.

En la figura 5.8 se muestra la actualización del proceso de marcado certificado. El PNDS puede implementarse con soluciones propietarias, pero se recomienda optar por soluciones que sigan la estructura de una PKI, lo que incidirá en la interoperabilidad y reúso de los certificados emitidos. Pueden existir varios PNDS y, siempre y cuando éstos se organicen jerárquicamente apoyándose en una arquitectura PKI, las diferentes PN en ellos registradas mantendrán la confianza.

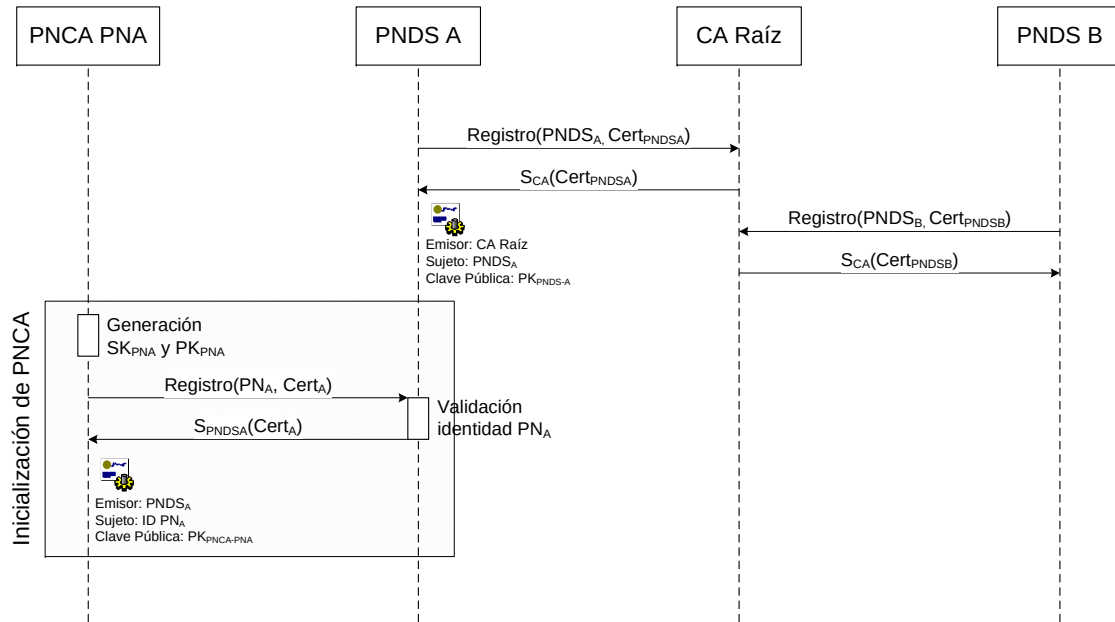


Figura 5.8: Adaptación del proceso de iniciación de la PNCA

El efecto de disponer de una CA común para todas las PN facilita la validación de los participantes en una PN-F, incluido el creador, en cualquier situación, ya sea una PN-F ad-hoc o soportada con la infraestructura. La revocación de nodos personales de cada PN deberá ser elevada ahora a un nivel superior para lograr el conocimiento por parte de cualquier PN. En este caso, procedimientos distribuidos como el planteado en el capítulo 4 no son sencillos de llevar a la práctica y no garantizan la distribución universal de las CRL, por lo que vuelve a ser recomendable el empleo del PNDS para estas tareas. No obstante, en situaciones completamente ad-hoc no existe otra alternativa. Con el soporte de una CA común, cualquier nodo personal que haya sido revocado automáticamente también dejaría de formar parte de la PN-F, siendo los propios nodos personales los que impedirían la comunicación con los nodos revocados. En cierta manera, la PN-F, dependiendo de la implementación que se realice, seguiría siendo segura.

El PNDS, como su propio nombre indica, hace también de almacén de la información de todas aquellas PN bajo su control. El hecho de disponer de este repositorio central permite plantear la publicación de pequeñas descripciones de cada PN en el momento de su registro. Esto facilita la identificación de las PN más allá de su nombre o alias y la búsqueda de potenciales socios a la hora de plantear una PN-F.

De este modo, cobra sentido que el PNDS sea la entidad que aloje los perfiles de las PN-F públicas, convirtiéndose en el punto de contacto donde los usuarios tratarán de localizar aquellas PN-F que puedan ser de su interés. El PNDS dispondrá de un motor de descubrimiento similar al incorporado en la SMP pues, abstrayendo los conceptos, las PN-F son servicios con unas condiciones muy particulares.

5.3.1.2. Evaluador de políticas

A diferencia de otras redes colaborativas, en la PN-F la influencia del contexto queda patente, ya que las condiciones de colaboración no son estáticas, sino que pueden variar durante su vida y su definición debe ser cercana al usuario. Para poder implementar esta nueva metodología de control de acceso y participación se requiere de motores cognitivos de razonamiento y decisión que incluyan la lógica necesaria para interpretar y analizar la información semántica vinculada a las políticas de la PN-F.

El PE actúa como intérprete de las reglas y políticas declaradas en los perfiles de la PN-F y valida las peticiones cruzando los datos de éstas contra los perfiles de participación y de la PN-F, concediendo o denegando el acceso. Dado que gran parte de los datos para tomar la decisión óptima (ontología de definición de políticas, perfiles, contexto, etc.) se aloja en la SCMF, el PE se encuentra estrechamente ligado a ella. De hecho, para la adaptación de la SCMF al entorno de la PN-F, se requiere establecer una mayor cohesión entre el CASM y el PE.

La figura 5.9 detalla los componentes que forman parte del PE. Al recibir una petición, el procesador de peticiones la analiza y disecciona, traducéndola al lenguaje natural de políticas. De ella se extrae la información de los papeles que juegan tanto el solicitante como el receptor de la petición y se traduce a una de las tres posibles relaciones, creador-miembro, miembro-creador o miembro-miembro. Esta información se toma como entrada del motor de decisión. Adicionalmente y provenientes de la SCMF, la información del contexto, los perfiles de usuario y las políticas se unen como variables de entrada a procesar. Las actualizaciones en estos valores alojados en la SCMF para la toma de decisiones deben propagarse al PE manteniendo la coherencia en su representación. Dado que la SCMF no comparte la misma representación semántica de la información que el PE, se define el actualizador como un componente intermedio que realiza las labores de monitorización de cambios y ajuste de esos datos.

Una vez que todos los datos están alojados en el espacio de decisión, se invoca al motor de razonamiento y decisión con esa información semántica como entrada. La respuesta se formatea y empaqueta de vuelta hacia la entidad que realizó la consulta, bien el FM, el CASM, etc.

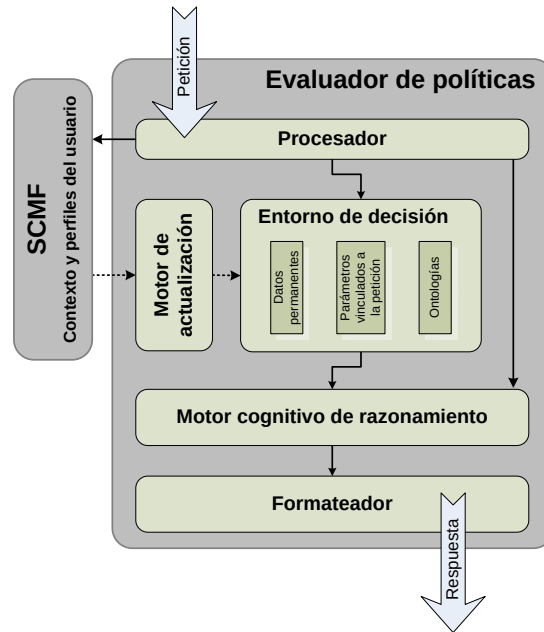


Figura 5.9: Arquitectura del PE

5.3.1.3. Asistente de federación

El FM se incluye en una PN-F como la entidad encargada de guiar a su PN durante el proceso de constitución de una PN-F. El FM es el componente central empleado para crear, controlar y mantener el vínculo de una PN con una o varias PN-F. Existe un FM por cada PN y trabaja independientemente de que las PN-F sean ad-hoc o basadas en infraestructura.

Una PN puede participar simultáneamente en varias PN-F, lo que hace que el FM deba mantener el estado en el que la PN se encuentra en cada una de esas PN-F. En este sentido el FM es el encargado de gestionar las transiciones entre los estados definidos en la figura 5.5. Se podría establecer la correspondencia directa entre las etapas del ciclo de vida y la máquina de estados que incorpora el FM, dado que el FM debe actuar tanto de creador como de participante y buscar un modelo más simplificado que trasladar al usuario de cada PN. No obstante, manteniendo la vinculación, se prefiere reducir a tres estados: en espera, en uso y PN-F desactivada. En la figura 5.10 se presenta el flujo de transiciones entre ellos.

Además de esta función, el FM contribuye en las tareas de generación, almacenaje, distribución y mantenimiento de los perfiles de la PN-F, en las que la PN actúa como creador, como los de participación.

Para hacer frente a todos estos cometidos, se define la arquitectura del FM tal como se refleja en la figura 5.11. En función del estado, el FM redirige o trata internamente cualquier primitiva de gestión de una PN-F. El FM interacciona así con:

- Nodos pasarela: para mediar en la formación de la PN-F.
- PE: para corroborar la correcta aplicación de las políticas.

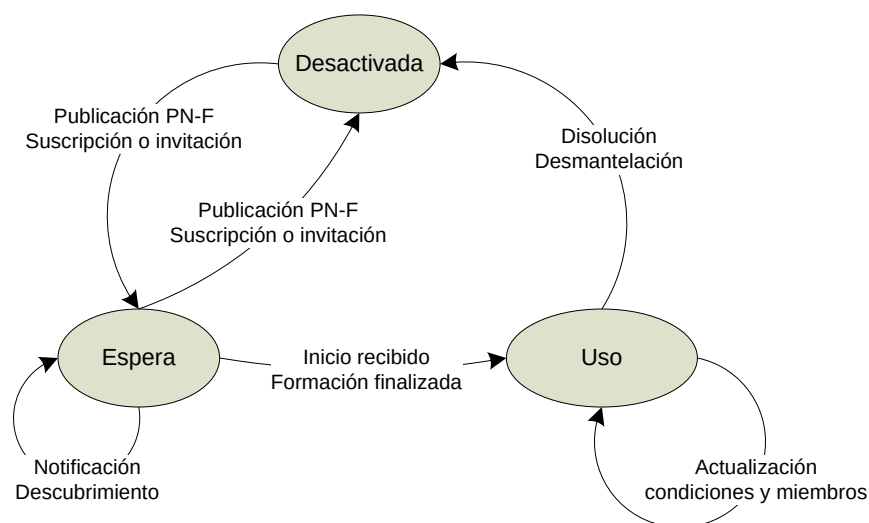


Figura 5.10: Máquina de estados simplificada del FM

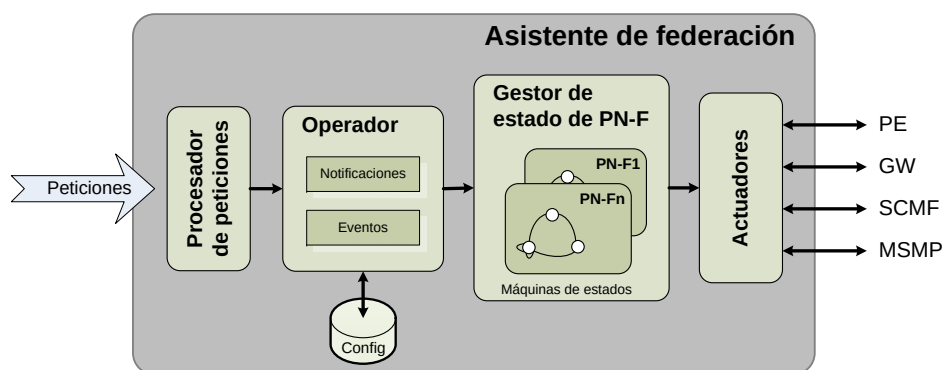


Figura 5.11: Arquitectura del FM

- FM remoto: para intercambiar información de control dentro de la PN-F.
- SMP: para informar a las otras PN de las características de la red superpuesta de servicios.
- SCMF: para suscribirse a cambios en el contexto o administrar la información de perfil o políticas de uso.

5.3.2. PN-F sobre red virtual

Siendo la PN una red privada virtual orientada a facilitar la interacción de un usuario con sus dispositivos y servicios, la idea de extender las soluciones desplegadas para hacerla realidad al caso de una PN-F, donde los dispositivos y servicios personales de varios usuarios interaccionan, y plantear la PN-F como una red privada virtual entre usuarios no parece disparatado. Esta opción permitiría no sobrecargar con nuevas funcionalidades a los nodos y reusar lo máximo posible las metodologías y protocolos ya diseñados para el caso de la PN.

En la figura 5.12 se ilustra el concepto de redes virtuales superpuestas para desplegar las PN-F. Cuando un grupo de personas se quieren federar, establecen una red virtual entre los dispositivos y nodos de sus respectivas PN. Algunos de esos dispositivos proporcionarán servicios u otros recursos, otros sólo se emplearán para establecer la conectividad necesaria y algunos, a voluntad del dueño de la PN especificándolo en su perfil de participación, podrán quedar fuera de la federación. Este aspecto es especialmente relevante, pues compartir un servicio no implica que se abra completamente el nivel de red para dar el acceso a él. Indicar, como aspecto adicional, que el hecho de restringir el uso de los nodos personales dentro de una PN-F, aparte de impedir el conocimiento y acceso a ellos y sus servicios, tiene como objetivo impedir la degradación del tráfico personal.

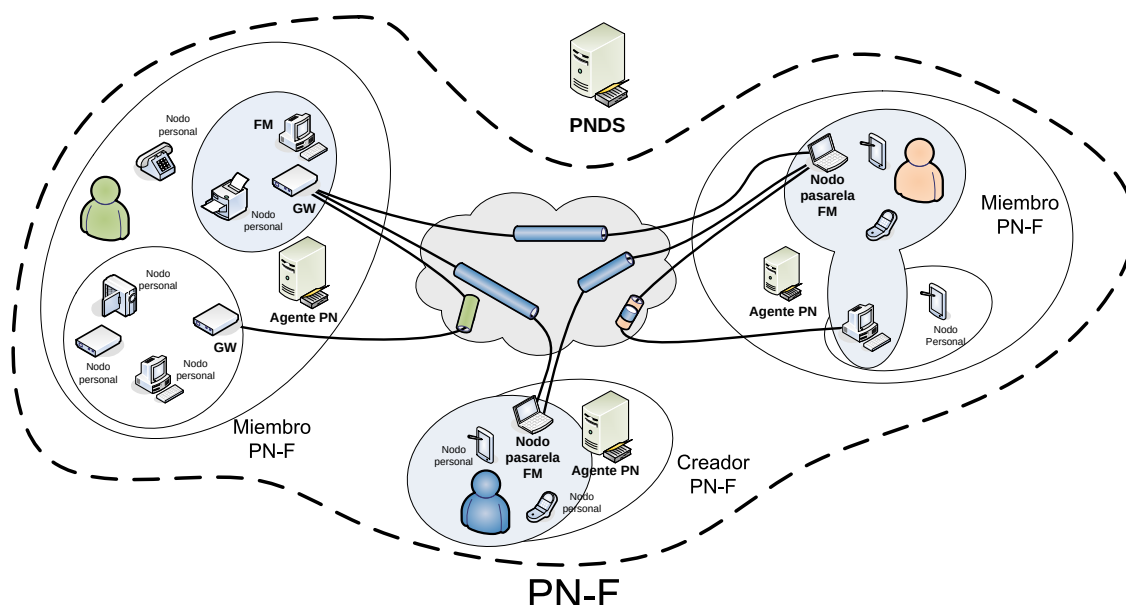


Figura 5.12: PN-F como red virtual a nivel de red

Para separar el tráfico personal del generado en el ámbito de la PN-F, cada PN-F tendrá su propio espacio de direccionamiento. Así pues, los nodos personales tendrán, además de la dirección personal y la dirección pública (en el caso de los nodos pasarela), una dirección única por cada PN-F en la que participen.

Aunque todo el tráfico quede confinado dentro de la PN-F, la información debe viajar cifrada y autenticada. La implantación de una PN-F sobre redes virtuales emplea el modelo descrito en el capítulo 4, donde a partir de las claves bilaterales, en este caso con una validez limitada a la vida de la PN-F, los nodos conforman canales seguros entre ellos en los diferentes niveles. Por tanto, la UCL y los túneles dinámicos extienden su operativa a la PN-F.

Al igual que en la PN, la red virtual soporta tanto PN-F en infraestructura como en modo ad-hoc. A continuación, siguiendo la evolución de una PN-F a lo largo de su ciclo de vida, se plantea la interacción de los diversos componentes funcionales y la adaptación a la PN-F de las funcionalidades, protocolos, etc. definidos para la PN. Adicionalmente se definen nuevas características propias de la PN-F. Sirvan como introducción y como guía de

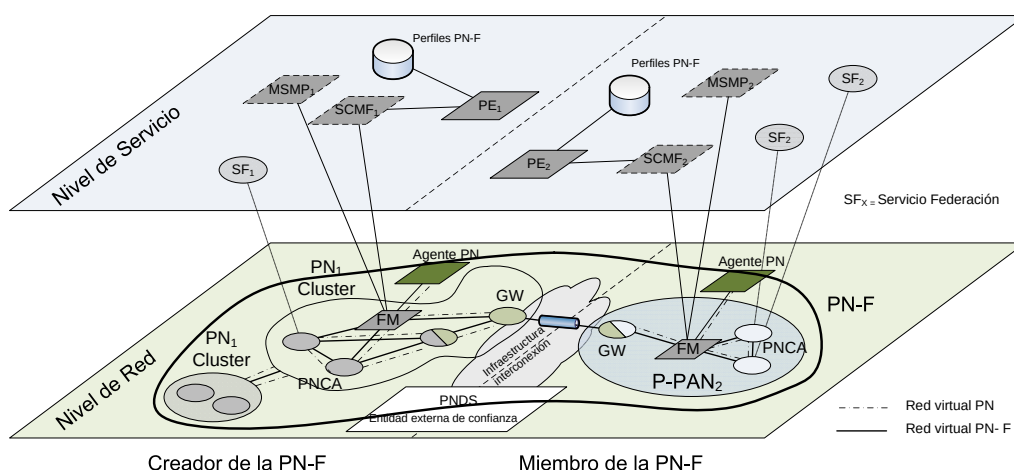


Figura 5.13: PN-F sobre red virtual sustentada en infraestructura

las posteriores descripciones los diagramas de las figuras 5.13 y 5.14, en los que se representa la visión global de ambas soluciones.

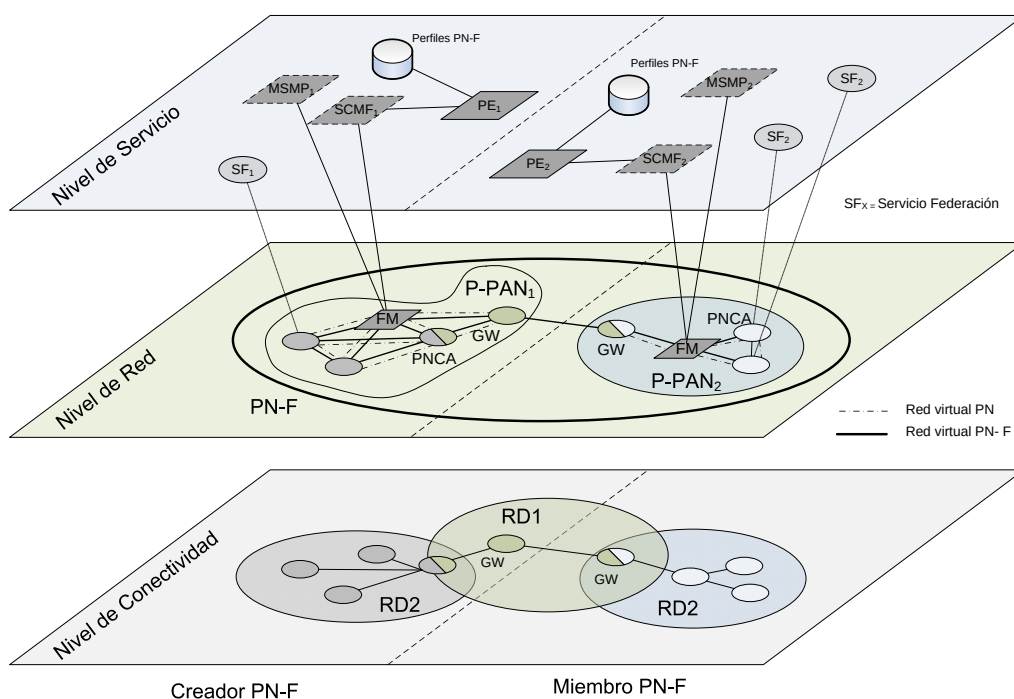


Figura 5.14: PN-F ad-hoc sobre red virtual

5.3.2.1. Publicación y descubrimiento

Tal como se ha venido comentando, básicamente existen dos métodos para lanzar el proceso de participación en una PN-F: invitación o suscripción. Ambos procesos sólo se diferencian en el primer paso, es decir, la forma en la que se descubre la PN-F y se tiene acceso al perfil definido por el creador.

5.3.2.1.1. Infraestructura

Sustentándose en la confianza que ofrece el PNDS, el creador publica el perfil de su PN-F en él, mientras que las PN en búsqueda de PN-F de interés se suscriben también en el PNDS haciendo público un perfil genérico de participación. En la figura 5.15 se muestra tanto el proceso de publicación como el de suscripción/invitación. Para mantener la explicación más simple se considera que tanto los creadores como los potenciales miembros comparten el mismo PNDS.

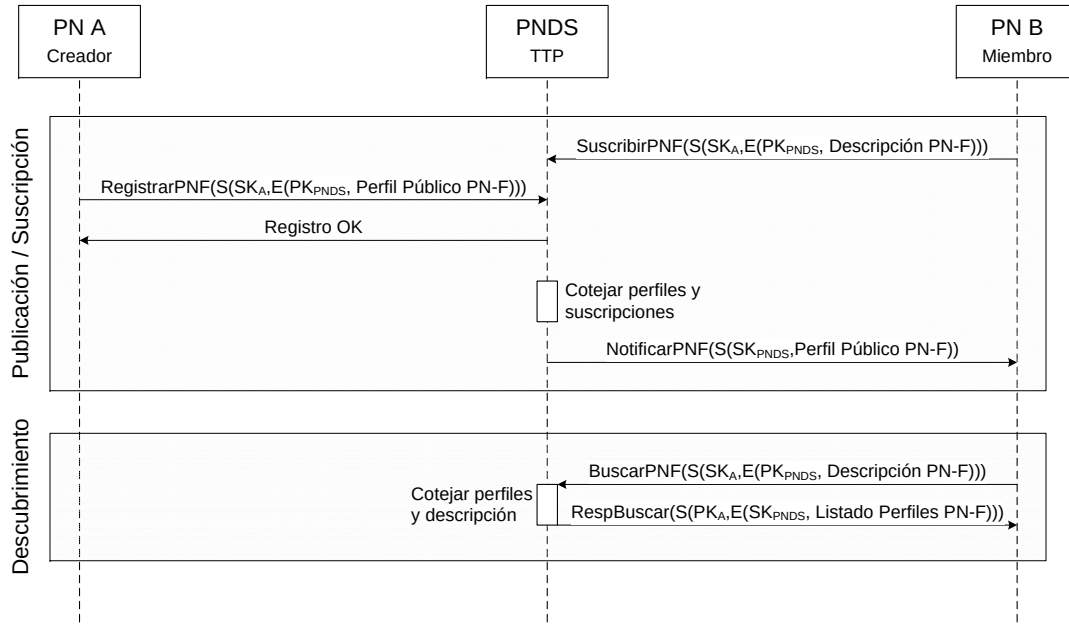


Figura 5.15: Publicación y descubrimiento de PN-F en modo infraestructura

En el proceso de publicación el creador firma la parte pública del perfil de la PN-F y cifra la primitiva de publicación conteniendo todo el mensaje, aunque esto último no es obligatorio. A su recepción, el PNDS valida la identidad del publicador y confirma el correcto registro de la PN-F. La información mínima a incluir, a partir de lo descrito en el apartado 5.2.1.1, incluye la identidad del creador, el punto de contacto y las condiciones de activación.

Si existiera alguna PN que previamente se hubiera suscrito a la publicación de PN-F con un propósito similar, el PNDS se pondrá en contacto con ella haciendo uso de la información de contacto incluida en el perfil de participación cedido.

Estos procesos pueden estar totalmente desligados, desembocando en la búsqueda activa bien por parte del creador de PN a las que invitar o bien por una PN cualquiera de PN-F de interés.

5.3.2.1.2. Ad-hoc

El caso ad-hoc muestra como principal diferencia la falta de acceso al PNDS como repositorio de PN-F. Por el contrario, los creadores de PN-F deben difundir y publicitar sus

PN-F de forma autónoma, bien mediante la interacción directa con los dueños de otras PN o bien empleando procedimientos de red, como se describe en la figura 5.16.

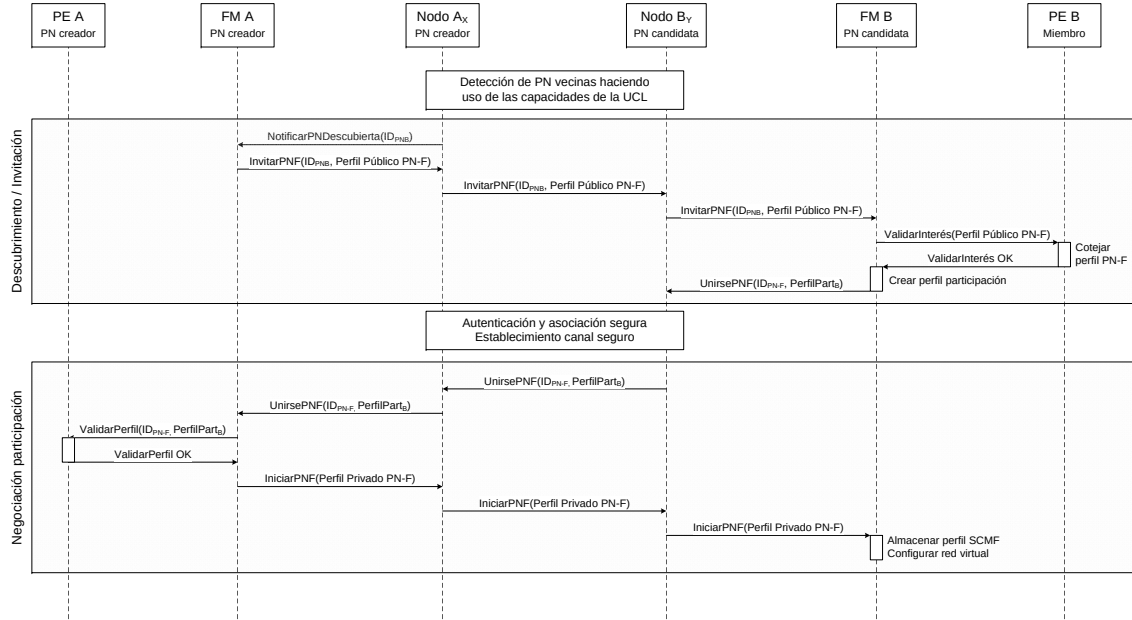


Figura 5.16: Publicación y descubrimiento de PN-F en modo ad-hoc

Los nodos de la PN del creador detectan la emisión de mensajes de difusión con otro identificador de PN, ante lo cual instan al FM a publicitar las PN-F disponibles mediante invitaciones incluyendo el perfil de la PN-F autenticado. Las PN vecinas recogerán esa información para comprobar si se ajusta a sus intereses e iniciar así la colaboración.

De modo complementario, toda PN puede instar a su FM a lanzar mensajes de búsqueda, que serán respondidos con invitaciones personalizadas en caso de existir alguna PN-F activa en el área. Esas invitaciones irán dirigidas al punto de contacto de la PN solicitante, que las remitirá al FM correspondiente para su evaluación.

Uno de los mayores retos a los que se enfrentan las PN-F ad-hoc es el establecimiento de un canal físico de comunicación entre los nodos de diferentes PN, es decir, tienen que compartir al menos un DR. Antes de emprender la participación y formación de la PN-F este aspecto ha tenido que ser resuelto.

Tanto los conceptos de PN como de PN-F se basan en la auto-configuración sin necesidad de requerir la interacción del usuario. Para el caso de la PN, hacer frente a esta problemática sólo involucra a un usuario quien instaba a todos sus nodos a compartir un mismo canal dependiendo de la tecnología radio empleada. Sin embargo, en el caso de las PN-F, la cuestión no resulta tan trivial dependiendo de la tecnología de comunicaciones. En el caso de emplear Bluetooth, definir un máster común de la picored solventa la comunicación entre dos islas de dos usuarios. Incluso el descubrimiento o publicación de la PN-F se puede hacer empleando los procedimientos propios de Bluetooth.

Otra tecnología extendida en los entornos de PAN es IEEE 802.11. Los nodos de los *clusters* basados en ella comparten modo de operación, *Independent BSS* (IBSS) o *Basic*

Service Set (BSS), e identificador de red o *Service Set Identifier* (SSID). Empleando los mecanismos propios de descubrimiento de red disponibles se puede dar soporte principalmente al caso IBSS, pues los nodos compartirían un coordinador y conectándose a él obtendrían el vínculo a nivel de enlace. En las redes IEEE 802.11 ad-hoc puras, la figura del coordinador no existe como tal y ahí se necesitan procedimientos de sincronización y distribución mucho más complejos que necesitarían de entidades adicionales. No obstante, en cualquiera de los casos, antes de cambiar el SSID, las PN deben estar seguras no sólo de la identidad de las vecinas con las que van a compartir conexión, sino sopesar los beneficios que conllevaría la reconfiguración de todos los nodos de su *cluster* local, que suele coincidir con la P-PAN.

Actualmente el *hardware* IEEE 802.11 soporta la generación de varias celdas con SSID diferentes, permitiendo la interconexión entre ellas con pequeñas modificaciones en las tablas de rutas. Si bien la interferencia entre ellas puede ser superior, la degradación de la QoS compensa la mejora en la QoE.

En el ámbito de esta tesis, no se ha estudiado en profundidad la solución a esta problemática por requerir análisis y desarrollos sobre los niveles físicos de las diferentes tecnologías de red. En las validaciones realizadas de las PN-F ad-hoc se ha supuesto que los usuarios comparten o han acordado un SSID para configurar sus redes.

5.3.2.2. Asociación

Hasta este punto de la fase de participación, las PN sólo pueden considerar como autenticada la interacción con el PNDS. Si bien confían en la información transmitida en los perfiles dado que está autenticada a partir de un certificado emitido por el PNDS, los nodos que interactúan no tienen la certeza de que el otro extremo es de confianza e incluso en algunos casos puede no haberse registrado en el PNDS.

Para poder proseguir, el creador y los candidatos deben autenticarse mutuamente y negociar los parámetros necesarios para establecer una asociación segura entre ellos. De este modo se garantiza la seguridad del resto de los pasos de una PN-F. Considerando los escenarios ligados a una PN-F, se plantean dos métodos de autenticación. El primero, enfocado principalmente a las PN-F basadas en infraestructura, se apoya en la relación de confianza en una TTP, en este caso el PNDS, establecida con anterioridad. En este caso, ambas PN pueden emplear procesos estándar para probar la posesión de la clave privada vinculada a los certificados, tales como TLS. No obstante, buscando homogeneizar las soluciones de seguridad de la PN y las PN-F, se recomienda emplear el procedimiento descrito para la segunda etapa del CPFPP que, además de operar sobre canales no seguros a cualquier nivel, habilita un conjunto de claves bilaterales a largo plazo para asegurar los intercambios entre las PN.

El segundo, sin el soporte activo en una TTP, emplea el concepto de PAC y la participación activa de los usuarios involucrados en la PN-F. La ejecución del proceso de validación empleando el PAC mantiene el planteamiento establecido para las PN, tanto para el caso de PAC público como privado. Suponiendo un procedimiento de invitación, en la figura 5.17 se muestra el intercambio de mensajes entre los nodos. Se aprecia que ahora los usuarios, usualmente por parejas, interaccionan. Por ejemplo, en el caso de un PAC privado uno de

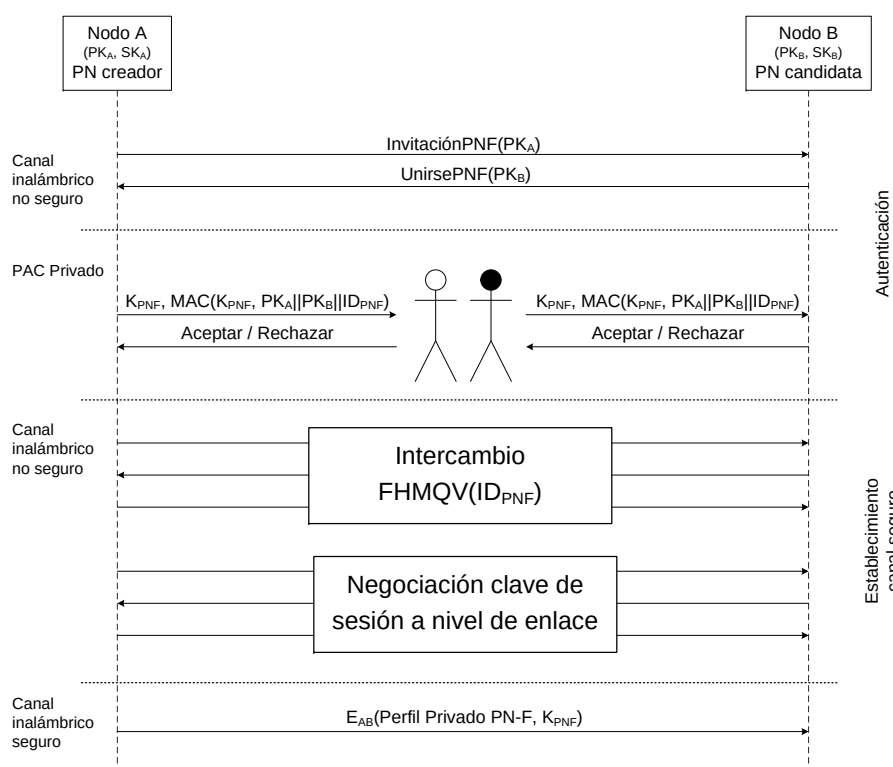


Figura 5.17: Proceso de autenticación y derivación de claves en PN-F ad-hoc

ellos muestra la clave de autenticación al otro, quien la introduce en su dispositivo; esto supone que los usuarios están presentes y se conocen.

El CPFP se diseñó para personalizar nodos de un usuario. Para extender la confianza que otorga su uso a la PN-F y lograr vincular esta relación a una única PN-F, se debe modificar el CPFP para incluir el identificador de la PN-F como variable de entrada a la función de derivación. De otra forma, la confianza que se hubiera establecido entre los nodos de múltiples PN sería genérica y las claves generadas se podrían emplear en PN-F comunes independientemente de las políticas de cada una.

Tras la autenticación, los nodos empleados para presentar ambas PN (comúnmente los nodos pasarela) establecen el canal seguro siguiendo unas pautas similares a las de la PN, pero en este caso empleando las claves bilaterales resultado del proceso anterior. Es entonces cuando se intercambian información más detallada de los perfiles de participación, que será redirigida al correspondiente PE para su validación. Hasta que no se finalice el proceso de formación, la confianza, aunque establecida a nivel PN, sólo se mantiene entre los nodos que han participado en esta primera toma de contacto. A partir de ese momento, la confianza, es decir, claves bilaterales, etc. se difundirá a todos los nodos involucrados en la PN-F.

5.3.2.3. Formación

Autenticadas las dos PN y establecido el canal seguro que permita proteger los intercambios, se da por concluida la fase de participación, iniciándose la de formación con la solicitud por parte de la PN candidata de formar parte de la PN-F.

Sobre el canal seguro, el FM del potencial miembro envía su perfil de participación, ajustado según su criterio a las condiciones establecidas por el creador. El FM del creador redirige el perfil de participación al PE quien analizará el correcto ajuste de sus características al perfil de la PN-F. En caso que el perfil de participación no se adecue, se procederá a una negociación entre las dos PN para buscar un acuerdo. Esta negociación se puede realizar de forma automática entre los PE según los ajustes preestablecidos por el usuario, pero también puede requerir la interacción de éste, quien adaptará el conjunto de recursos a compartir de forma manual.

Si el perfil de participación es válido, el PE del creador lo notifica al FM. Puede ocurrir que, aunque el perfil sea válido, las condiciones para iniciar la PN-F no se cumplan, bien porque aún no se ha unido algún participante, bien porque tiene un inicio retardado, etc. En esos casos, junto con la confirmación, se remite la información adicional. Posteriormente, se difundirá una actualización del estado de la PN-F a todos los miembros.

En el mensaje de inicio, el FM de la PN creadora remite a su homónimo en la otra PN la información incluida en la parte privada del perfil. Entre otras cosas, adjunta la lista de miembros actualizada y los puntos de contacto con ellos, datos del esquema de direccionamiento a emplear dentro de la PN-F y la descripción extensa de los servicios ofertados dentro de la PN-F (protocolos, localización, etc.). La parte privada del perfil de la PN-F comprende también la clave de difusión a emplear dentro de la PN-F. Este dato es especialmente sensible, ya que en caso que un miembro abandone la PN-F hay que generarlo y distribuirlo nuevamente.

El FM receptor se encarga de retransmitir la información a los nodos de su PN que participen en la PN-F. Definido el esquema de direccionamiento en la parte privada del perfil de la PN-F, cada PN es responsable de distribuir dicha información e instar a sus nodos a adoptar la nueva dirección dentro de la PN-F. Cada uno de estos nodos actualizará las tablas de rutas correspondientes para permitir al protocolo de encaminamiento determinar el camino más óptimo dentro de la PN. A la hora de establecer una ruta dentro de la PN-F, se puede fijar como métrica adicional la participación en la PN-F, acotando el conjunto de nodos intermedios para cualquier comunicación o servicio dentro del ámbito de la PN-F. Este modo de funcionamiento incrementa la seguridad en la PN-F al restringir el acceso a la información a nodos externos a ella, aunque en ocasiones puede provocar que, especialmente en PN-F espontáneas, no se encuentre una ruta. En esos casos, el establecimiento de túneles a nivel de red entre los extremos garantizaría la privacidad de las transmisiones. No obstante, por definición, todos los nodos de una PN son confiables, por lo que usarlos como puentes no debería suponer un riesgo de seguridad de la PN-F; es más, el usuario podría actualizar su perfil de participación para incluirlos.

Desde este punto, la formación de la PN-F difiere notablemente de una PN-F sobre infraestructura a una ad-hoc. Es por esto que a continuación, tras analizar los posibles esquemas de direccionamiento, se exponen cada una de las soluciones de forma individual.

5.3.2.3.1. Esquemas de direccionamiento

El concepto de red virtual superpuesta se apoya en el uso de un esquema de direccionamiento propio que permita identificar a los nodos en la nueva red. Los nodos personales que participen en la PN-F serán los que formen la red virtual y, por tanto, deben disponer de un identificador en la nueva red generada.

A nivel de red se asignan nuevas direcciones, pertenecientes a un nuevo espacio privado independiente del espacio de direcciones públicas y del asignado a la PN, lo que junto con la relación de confianza propia, evita conflictos entre el tráfico PN y el tráfico PN-F. Existen diversas posibles soluciones para definir el esquema de direccionamiento dentro de la PN-F, ambos compatibles con IPv4 e IPv6:

- Autónomo/Independiente: no mantiene ningún vínculo con el direccionamiento privado de las diferentes PN y puede considerarse ortogonal a ellos.

$$\text{Dirección PN-F} = \text{Prefijo PN-F} \mid \text{Sufijo único}$$

El dueño de la PN-F genera el prefijo y lo distribuye dentro del perfil de la PN-F. Dicho prefijo puede tomarse como un valor aleatorio, pero, en caso necesario, se puede implementar un mecanismo de asignación con resolución de direcciones. En el caso de PN-F publicadas en el PNDS será el propio PNDS quien detecte los prefijos duplicados.

- Jerárquico: la dirección de un nodo dentro de la PN-F se deriva de la dirección de asignada dentro de la PN a la que pertenece.

$$\text{Dirección PN-F} = \text{Prefijo PN-F} \mid \text{Prefijo PN} \mid \text{Sufijo único}$$

Una vez se selecciona el prefijo de la PN-F, todos los nodos quedan identificados de manera unívoca. Esto es así ya que, como se ha visto en el capítulo 3, la dirección PN es única. La aplicación de este esquema favorece el reúso de las tablas de encaminamiento intra-*cluster* existentes.

La primera solución permite ocultar la pertenencia de un nodo a una PN específica, considerando al nodo únicamente como parte de la PN-F. Por el contrario, la segunda sigue un paradigma jerárquico vinculado a la PN, lo que hace que la localización e identidad de los nodos esté más expuesta. Cualquiera de las dos soluciones planteadas ofrece las funcionalidades requeridas por la PN-F, lo que deja la elección de una u otra como una decisión a tomar en la implementación.

Destacar el hecho de que la elección del esquema de direccionamiento vinculado al identificador del nodo dentro de su PN permitiría mantener actualizada la información de rutas a nivel de *cluster* de una forma directa sin añadir sobrecarga de encaminamiento, ya que los datos coincidirían con los de la PN. En función del prefijo de la dirección destino se aplicarían bien las políticas de encaminamiento de la PN o de la PN-F.

Además del conjunto de direcciones propias para cada nodo, dentro de la PN-F se establece una serie de direcciones de difusión enfocadas a transmitir mensajes dirigidos a una PN en concreto, a varias o a todas la PN miembro.

5.3.2.3.2. Infraestructura

El establecimiento de la red virtual con apoyo de la infraestructura consta de una serie de etapas que se detallan seguidamente:

- Asignación de direcciones a los nodos de la PN-F.
- Enrutamiento intra-*cluster*.
- Determinar la localización de los otros *clusters* de la PN-F.
- Establecimiento de túneles dinámicos entre *clusters*.
- Enrutamiento inter-*cluster*.

Las dos primeras etapas son comunes tanto para redes ad-hoc como en infraestructura y dependen del esquema de direccionamiento seleccionado.

Para completar satisfactoriamente la formación de una red basada en infraestructura es imprescindible que los diferentes *clusters* conozcan la localización del resto de los *clusters* de la PN-F, tanto los de su propia PN como los del resto de los miembros. Tal como se refleja en la figura 5.18, los nodos pasarela de cada *cluster* serán los encargados de establecer el enlace, pero la confianza en los agentes de la PN será la que permita descubrir su localización, es decir, las direcciones de contacto públicas de los nodos pasarela de los *clusters*.

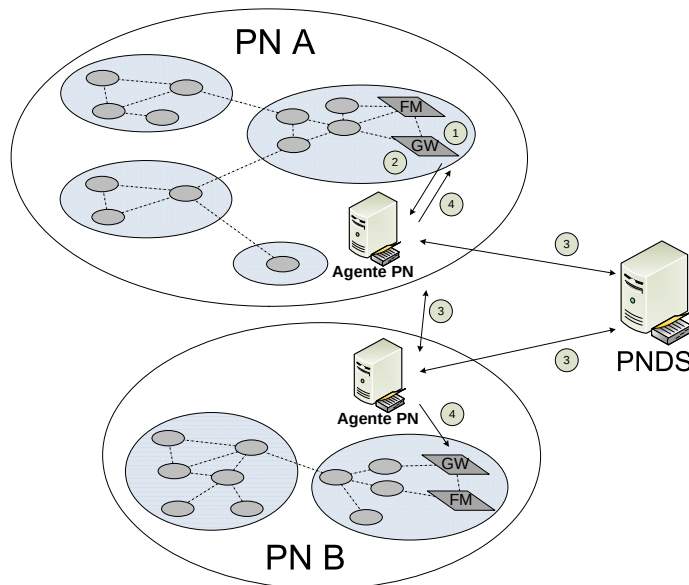


Figura 5.18: Descubrimiento de *clusters* en la PN-F

En este sentido, el FM remite la lista de PN miembros a los nodos pasarela que incluye los puntos de contacto de cada una. Lo más común es que ese punto de contacto se corresponda con el agente de la PN. Para evitar incurrir en el envío de múltiples solicitudes, los nodos pasarela emplean el agente de su propia PN, quien se pone en contacto con los otros agentes. La confianza entre los agentes está garantizada empleando certificados emitidos por el

PNDS. Existen diversas formas de llevar a cabo este procedimiento, de forma reactiva ante la solicitud por parte de los nodos pasarela, de forma proactiva o manteniendo una caché actualizada. De todas ellas, la última se presenta como la más eficiente al evitar tener que repetir el envío de la petición cada vez que un nodo pasarle lo solicita. Es más, una vez que un agente de la PN interroga a otros agentes de la PN podrá registrarse ante posibles actualizaciones de los perfiles de participación para PN-F específicas.

Toda vez que el agente de la PN obtiene la respuesta, la información es enviada de vuelta a los nodos pasarela, quienes inician el proceso de establecimiento de los túneles seguros entre *clusters*. El procedimiento seguido es similar al descrito para el caso de la PN. Sin embargo, en la PN-F el número de túneles a mantener puede incrementarse rápidamente debido al crecimiento del número de miembros. Para tratar de solventar este problema se plantean diversas soluciones. Por un lado, el uso de *routers* fronterizos facilitaría enormemente las tareas de mantenimiento en una PN-F dado que los nodos pasarela se verían liberados de esas funcionalidades, lo que supone una reducción de los recursos necesarios y consumidos. Si por el contrario, la PN no adopta el concepto de *router* fronterizo, la opción para reducir el consumo de recursos por parte de los nodos pasarela puede ser la reutilización de los túneles, es decir, emplear un mismo túnel para dar soporte a varias PN-F. La confianza final entre los nodos se proporciona gracias al PNDS y dado que todo el tráfico intra-PN-F se cifra con las propias claves de la PN-F se puede considerar que encapsularlo en otro túnel no supone un riesgo a la seguridad de la PN-F. Es más, aunque el túnel no se establezca ni se mantenga, sí se puede instar a los nodos pasarela a que se autentiquen y den la autorización de emplear otro túnel.

En este punto, la PN-F se puede dar por constituida funcionalmente al estar los canales de comunicación entre los nodos establecidos. Aunque en la definición de la PN y durante su evaluación se analizaron varios protocolos de encaminamiento, la implementación de una PN debe apoyarse únicamente en uno. Así se podrá extender ese protocolo con las métricas necesarias para su uso en la PN-F. De otra forma, la negociación de la participación en la PN-F implicaría también tener que pactar la forma de comunicación.

Dentro de la PN-F se recomienda emplear métricas de encaminamiento basadas en las políticas definidas en el perfil de la PN-F y en los de participación [188]. Esto permitirá una mayor granularidad en el control de acceso a los nodos, incluyendo filtros o *firewalls*, etc.

5.3.2.3.3. Ad-hoc

La formación de una PN-F ad-hoc sigue un proceso similar al empleado en las redes sustentadas en infraestructura que se ha descrito anteriormente, pero eliminando los procesos que involucran las comunicaciones con *clusters* o nodos remotos (establecimiento de túneles, descubrimiento de agentes de la PN, etc.) y extendiendo los procedimientos intra-*cluster*.

La principal diferencia se observa en la forma de establecer la confianza entre los *clusters* de una PN-F ad-hoc, ya que, aunque también se basa en los certificados firmados por el PNDS, dado que en ellas no se puede realizar una validación en tiempo real, será el usuario quien tenga la última palabra mediante el uso del PAC.

Distribuida la información de direccionamiento y configuradas las tablas de rutas de los

nodos, la fase de formación se puede dar por concluida. El protocolo de encaminamiento se encargará de determinar las rutas seguras más óptimas.

5.3.2.4. Utilización de los servicios

Finalizada la fase de configuración y despliegue de la red virtual, todo el tráfico de la PN-F queda confinado de forma segura dentro de dicha red. Es ahora cuando se procede a compartir el uso de los servicios que han sido el objeto de la creación de la PN-F.

El FM, a través de los perfiles de participación y de la PN-F, conoce los detalles de la PN-F y, en colaboración con las SMP de cada PN, pone los servicios disponibles en conocimiento del resto de los nodos que forman parte de la PN-F. Los SMN distribuyen la información dentro de cada *cluster* y mediante la red virtual de SMN se logra extenderla a todo el rango. Los procesos de descubrimiento de servicios siguen el mismo mecanismo que para el caso de la PN pues, como ya se ha insistido, una vez formada la PN-F la operativa es similar a la de la PN. La principal diferencia se produce en los procesos de sincronización del listado de servicios, en la autenticación y en la validación de la provisión del servicio donde además de considerar el contexto se deben tener en cuenta las políticas impuestas por los perfiles. Para estas tareas, el SMN se apoya en su SCMF, que evalúa las condiciones de la petición con el perfil de participación. Así, del mismo modo que se restringió el hecho de que ciertos nodos actuaran como nodos intermedios en las comunicaciones multisalto, los servicios se harán visibles sólo a los nodos de la PN-F. La figura 5.19 muestra todo este proceso.

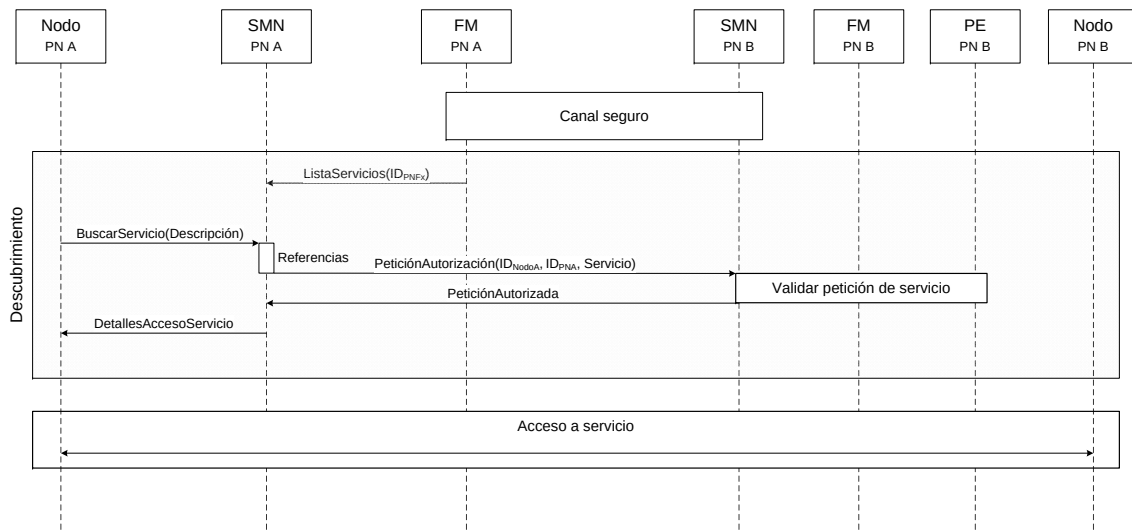


Figura 5.19: Uso PN-F en modo ad-hoc

La provisión de los servicios se realiza extremo a extremo entre los nodos implicados, siempre y cuando cumplan con las condiciones de acceso.

5.3.3. PN-F empleando un intermediario de servicios

El objetivo principal de una PN-F es compartir de forma segura una serie de recursos entre usuarios. Tomando como base la PN, la PN-F busca simplificar los procesos de esta-

blecimiento y mantenimiento de la relaciones entre PN. En este sentido, los recursos por los que los usuarios muestran especial interés son los servicios, es decir, funcionalidades de alto nivel que, abstrayendo todos los procesos subyacentes de conectividad, ofrezcan la utilidad requerida. Por tanto, cobra sentido plantear una PN-F basada únicamente en servicios considerando que, *de facto*, las capacidades de comunicación necesarias existen y operan correctamente y que no se requiere el establecimiento de una nueva relación entre todos los nodos de las PN participantes.

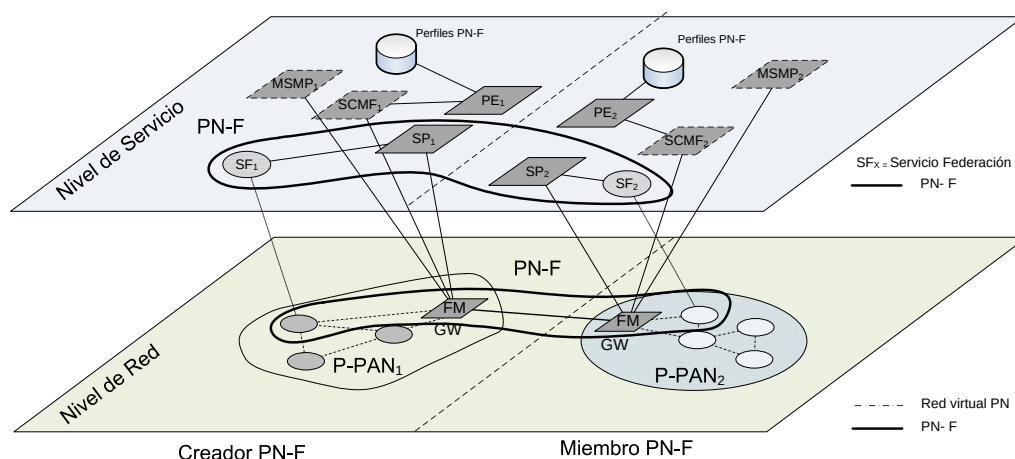


Figura 5.20: PN-F empleando un intermediario de servicios

En la figura 5.20 se representa el despliegue de una PN-F basada en los servicios. Esta arquitectura, focalizada en la Capa de Abstracción a Nivel de Servicio, opera de forma independiente del nivel de red, siendo los servicios los únicos recursos accesibles. A las entidades funcionales definidas en la arquitectura genérica de una PN-F (FM, PE y PNDS) en este caso hay que añadir el intermediario de servicios (SP, *Service Proxy*).

El SP actúa como un nodo pasarela que gestiona la interacción con los servicios exportados por una PN, permitiendo el acceso y provisión a todos aquellos miembros que se han asociado (ver figura 5.21). Esta filosofía de operación permite separar totalmente el tráfico inter-PN del tráfico intra-PN, de forma que los nodos de cada PN, aun ofreciendo los servicios a nodos de otras PN en la federación, no apreciarán diferencias con la provisión dirigida a los propios nodos personales.

El SP se desdobra en múltiples representantes, uno para cada servicio exportado por la PN, que serán los encargados de administrar el ciclo de vida del servicio a su cargo. Todo cliente que acceda a un servicio abrirá un canal dedicado a través del representante. Será este último quien realice el acceso, trasladando los mensajes del nodo externo. En el caso más simple, el representante de un servicio aplicará NAT, autorizando y redirigiendo el tráfico de los puertos asignados al servicio en cuestión. La implementación se puede complicar considerando no sólo la redirección de tráfico, sino incluyendo la monitorización y análisis de los datos transmitidos buscando una gestión más precisa del servicio. Un claro ejemplo de esta situación es la redirección del tráfico cifrado en el acceso al servicio como el generado durante una sesión SSL. Dado que el acceso no se realiza extremo a extremo,

sino a través del SP, dicho SP deberá desencapsular la información cifrada y encapsularla sobre el nuevo canal seguro dentro de la PN.

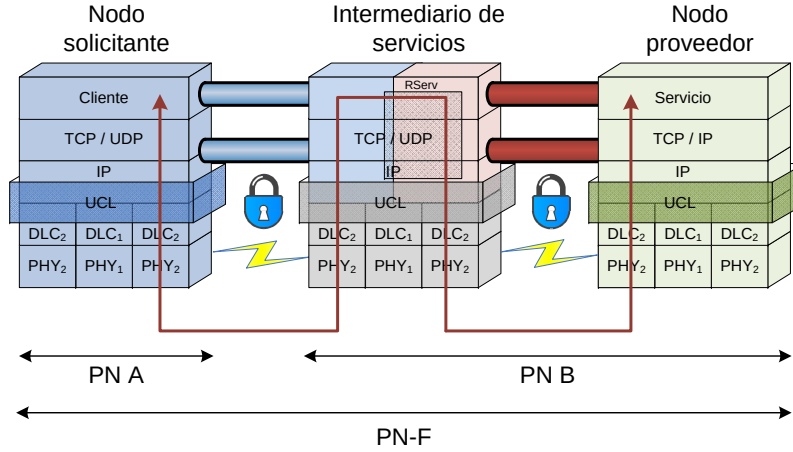


Figura 5.21: Flujo de información en una PN-F empleando un intermediario de servicios

El hecho de concentrar la gestión de la PN-F en la frontera de cada PN se erige como la principal ventaja del uso de la arquitectura basada en el SP. Por un lado, reduce el riesgo de accesos malintencionados ya que todo el tráfico externo se redirige a través del SP. Y por otro lado, al realizarse el registro, descubrimiento y provisión de los servicios a través de dicho SP, no es necesario modificar o incluir nuevas funcionalidades en los nodos de las PN federadas, pues todo el tráfico perteneciente a la PN-F se traduce en tráfico personal una vez atraviesa el SP.

Seguidamente se detalla el ciclo de vida de una PN-F basada en SP del mismo modo que se ha realizado para las PN-F basadas en redes virtuales. En este caso, las etapas de la PN-F tienen una correspondencia prácticamente directa con las del ciclo de vida de un servicio y así se observará en las descripciones posteriores. La figura 5.22 muestra el flujo de mensajes que se intercambian las diferentes entidades participantes en la PN-F, de forma que un usuario pueda descubrir y usar servicios ofertados por la PN de otro usuario.

5.3.3.1. Creación y asociación segura

Una PN-F se inicia con la definición, por parte del creador, de su perfil en el que se incluyen el objetivo, las funcionalidades, las políticas y las reglas que los miembros deberán cumplir. Usualmente es el FM de la PN creadora quien actúa como dirección de contacto.

La composición de los perfiles, su proceso de creación y su publicación siguen una metodología similar a la descrita para el caso de las PN-F basadas en redes virtuales, con la salvedad que en este tipo de PN-F los perfiles, tanto de participación como de la PN-F únicamente incluirán servicios, mientras que en el modelo anterior el usuario podía detallar incluso los dispositivos o nodos que participarían en la PN-F.

Una vez generados los perfiles, dependiendo de si se trata de una PN-F ad-hoc o una basada en infraestructura, serán bien el FM o el PNDS del creador el encargado de difundirlos o invitar a aquellas PN que desee.

Todas aquellas PN interesadas en formar parte de una determinada PN-F se deben asociar de forma segura cumpliendo con las reglas impuestas por el perfil de la PN-F. Las PN candidatas negociarán con el creador y el resto de los miembros los recursos (servicios) que pondrán a disposición de la PN-F y, haciendo uso de los procedimientos de seguridad, extendidos de la PN y descritos ya para la PN-F basada en infraestructura, habilitarán un canal seguro a través del cual autenticarse e intercambiar información.

5.3.3.2. Participación y formación

Durante la fase de participación y una vez que todas las partes han alcanzado un acuerdo en las condiciones de participación en la PN-F, cada PN registra los servicios ofertados con su punto de contacto, que, normalmente y como ya se ha comentado, coincide con el FM. Esta información será posteriormente empleada por la SMP, más concretamente por los SMN, para responder a las peticiones de servicios y determinar su localización.

Adicionalmente las PN proveedoras de servicios instan a su FM a generar un representante de servicio por cada uno de los servicios que presenten al exterior. La configuración del SP implica en estos casos definir tanto la dirección de contacto externa como la interna dentro de la PN.

En este sentido, se pueden considerar dos metodologías a la hora de registrar, crear y usar los representantes de servicio. Por un lado la opción reactiva, donde el SP instancia el representante en el momento que un determinado servicio va a ser utilizado. La opción proactiva supone que la instancia se realiza durante la fase de participación cuando el FM identifica los servicios que se comparten. Ambas opciones son válidas, si bien la opción reactiva al tiempo que permite no inmovilizar recursos que pueden no estar siendo utilizados facilita la adaptación en caso que la localización del servicio varíe.

5.3.3.3. Utilización de los servicios

Configurada la estructura que da soporte a las funcionalidades de la PN-F es el momento de formalizar los mecanismos de uso. Para ello se describen a continuación las fases de descubrimiento y provisión de un servicio. En el modelo basado en redes virtuales, donde la PN-F se podría considerar como la prolongación de una PN no sólo como concepto sino en su despliegue, las soluciones heredadas de la PN son válidas. Sin embargo, aunque las PN-F sustentadas en el SP comparten muchos de los procedimientos de las etapas iniciales con ellas, la filosofía de funcionamiento una vez está desplegada difiere notablemente.

Considerando la creación reactiva de los representantes de servicio, es decir, que la localización del servicio no se conoce de antemano, en la figura 5.22 se muestra el proceso de descubrimiento de un servicio dentro de la PN-F. Todo comienza con un usuario que quiere acceder a un servicio ofrecido por una PN remota dentro del ámbito de una PN-F. El primer paso es descubrir la localización del servicio, para lo que se hace uso de la SMP. El SMN local, tras determinar que el servicio lo ofrece otra PN, proporciona la dirección del SP local. Será éste quien, apoyándose en el FM, habilite el acceso al servicio remoto.

El FM local lanza la solicitud al FM remoto, quien tras validar la identidad del solicitante, interroga a su SMN. El SMN indica la dirección del dispositivo que ofrece el servicio. El SP toma las riendas de la comunicación con el nodo proveedor instanciando un representante.

Por su parte el FM envía la respuesta a la solicitud redirigiendo todo el tráfico que se genere a posteriori hacia el SP.

A partir de este momento se puede iniciar la provisión del servicio. A pesar de que se ha autenticado y autorizado al FM solicitante durante la fase de descubrimiento, dependiendo del servicio se requerirá también la validación para su uso. El PE y su análisis de los perfiles de participación acordados juegan un papel muy importante en este proceso.

Garantizada la seguridad en el acceso, la PN que actúa como cliente, empleando las interfaces definidas inicia el uso del servicio remoto. Aunque para ella pueda parecer que el servicio es completamente accesible, los recursos internos de la PN remota siguen estando ocultos. El representante del servicio es el que realmente accede al servicio, haciendo el intercambio y adaptando el tráfico externo al interno y viceversa. Como se ha venido insistiendo, se puede considerar que este modo de operación incrementa la seguridad dentro de la PN-F al independizar totalmente la PN-F de la PN, haciendo que el intercambio federado se produzca entre los nodos pasarela o SP.

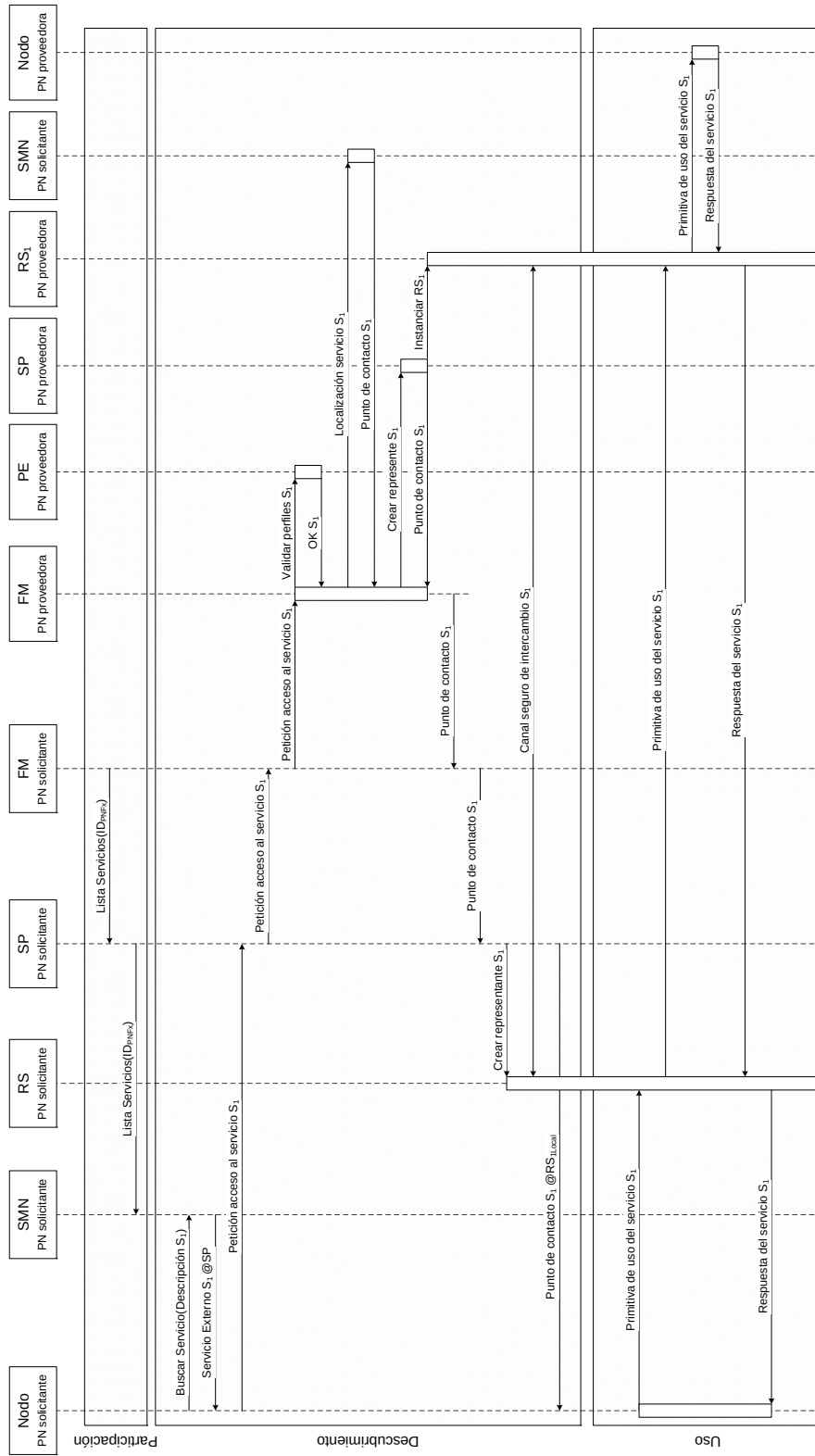


Figura 5.22: Secuencia de ciclo de vida de PN-F basada en SP

Capítulo 6

Validación experimental

Las redes y el equipamiento que las componen han sido, son y serán diseñadas por humanos con el objetivo de automatizar y facilitar las tareas del día a día. Sin embargo, el esfuerzo necesario para configurarlas y controlarlas escapa del conocimiento de la mayoría de sus usuarios; si bien es cierto que la vorágine tecnológica que envuelve a las nuevas generaciones ha despertado el interés por comprender la operativa de estas redes y los mecanismos de comunicación a través de ellas, en gran medida debido a que son las que habilitan el acceso global a la información.

No obstante, no se debe olvidar el objetivo principal para el que fueron diseñadas tanto las redes como sus equipos, era servir al usuario, aspecto éste aún no solventado hoy en día. Los usuarios saben qué redes y servicios se encuentran a su disposición, pero la reciprocidad no está resuelta, pues casi la totalidad de las redes desconocen las necesidades de sus usuarios y en muchos casos incluso no son conscientes de su existencia.

A lo largo de esta tesis se ha expuesto el concepto de una red con una clara orientación a dar servicio al usuario. Yendo más allá, se han planteado soluciones que permiten a los usuarios interaccionar entre sí e impulsar redes que den soporte a las necesidades no sólo de uno, sino de varios. En todos los casos, se ha hecho especial énfasis en el importante papel de la privacidad y la integridad en las comunicaciones.

Tanto las PN como las PN-F presentan numerosos retos en su especificación y aún más en su posterior implementación. Los primeros han sido abordados en los capítulos anteriores y resueltos en muchos de los casos con descripciones lo suficientemente detalladas como para favorecer su posterior evaluación. Los conceptos de PN y PN-F no deben estudiarse exclusivamente desde un punto de vista teórico o apoyándose en simulaciones que sustenten las especificaciones propuestas [120, 136]. Estas redes se han diseñado pensando en los usuarios y, por tanto, deben ser ellos quienes en última instancia las validen desde un punto de vista funcional, considerando el rendimiento y la usabilidad.

Evaluar la funcionalidad de una PN implica el despliegue de un número razonable de *clusters* con varios dispositivos o nodos de usuario en cada uno de ellos. Además, tanto una PN como una PN-F presentan una alta distribución de sus componentes, lo que supone que la implantación a realizar no debe circunscribirse a un entorno limitado de laboratorio, sino que, con el objetivo de analizar también las infraestructuras de red de los proveedores y

otros condicionantes, se precisa extender el área incorporando *clusters* situados en múltiples localizaciones.

Partiendo de estas premisas y tomando como base los escenarios y requerimientos que de éstos se extraen [89, 189], fruto del trabajo dentro del ámbito de los proyectos MAGNET y MAGNET Beyond, se procedió a la implementación de la PN y la PN-F en entornos reales [23, 72]. Los miembros del consorcio que lideraban las tareas de desarrollo, Universidad de Cantabria (UC) en España, Interdisciplinary Institute for Broadband Technology (IBBT) actualmente iMinds en Bélgica, Valtion Teknillinen Tutkimuskeskus (VTT) en Finlandia y el grupo GET del Institut National des Télécommunications (INT) en Francia, tal como se muestra en la figura 6.1, alojaron diversos *clusters* en sus instalaciones, interconectados a través de Internet, haciendo realidad una plataforma experimental el análisis de las PN y PN-F en condiciones reales.

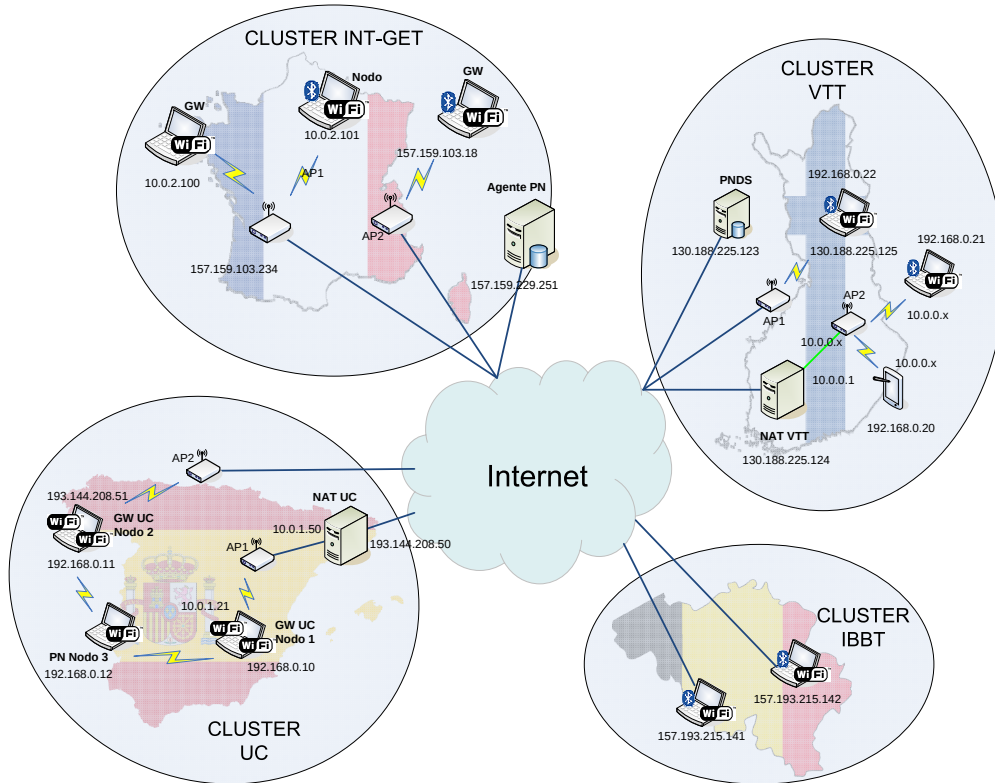


Figura 6.1: Despliegue del entorno de evaluación de PN y PN-F en MAGNET

Los *clusters* estaban formados por equipos de usuario comunes como ordenadores portátiles, teléfonos y PDA, una diversidad que permitiría demostrar realmente la viabilidad de la PN y la PN-F. Los desarrollos se realizaron sobre sistemas operativos basados en distribuciones Linux en todos ellos, como Ubuntu [190], para los terminales más potentes como ordenadores portátiles, o Maemo [191], para las PDA o tabletas seleccionadas (Nokia N770 [192] y Nokia N810 [193]).

Con la intención de facilitar aún más las tareas, y como parte del trabajo realizado

en esta tesis, todas las soluciones desarrolladas en el ámbito de estos proyectos, tanto las enfocadas a seguridad y comunicaciones, como las planteadas para dar soporte al contexto y provisión de servicios, se englobaron en una distribución de Ubuntu personalizada o *LiveCD* para portátiles y en una imagen de Maemo debidamente adaptada y configurada para su instalación en las tabletas de Nokia [185]. Ambas utilidades incluyen mecanismos de arranque y personalización amigables, lo que permite usar un nodo personal en cualquier dispositivo de la forma más simple posible y valorar su experiencia de uso, sin necesitar seguir complicados procesos de instalación y configuración, cumpliendo así con uno de los principales requisitos de la PN, la sencillez de uso.

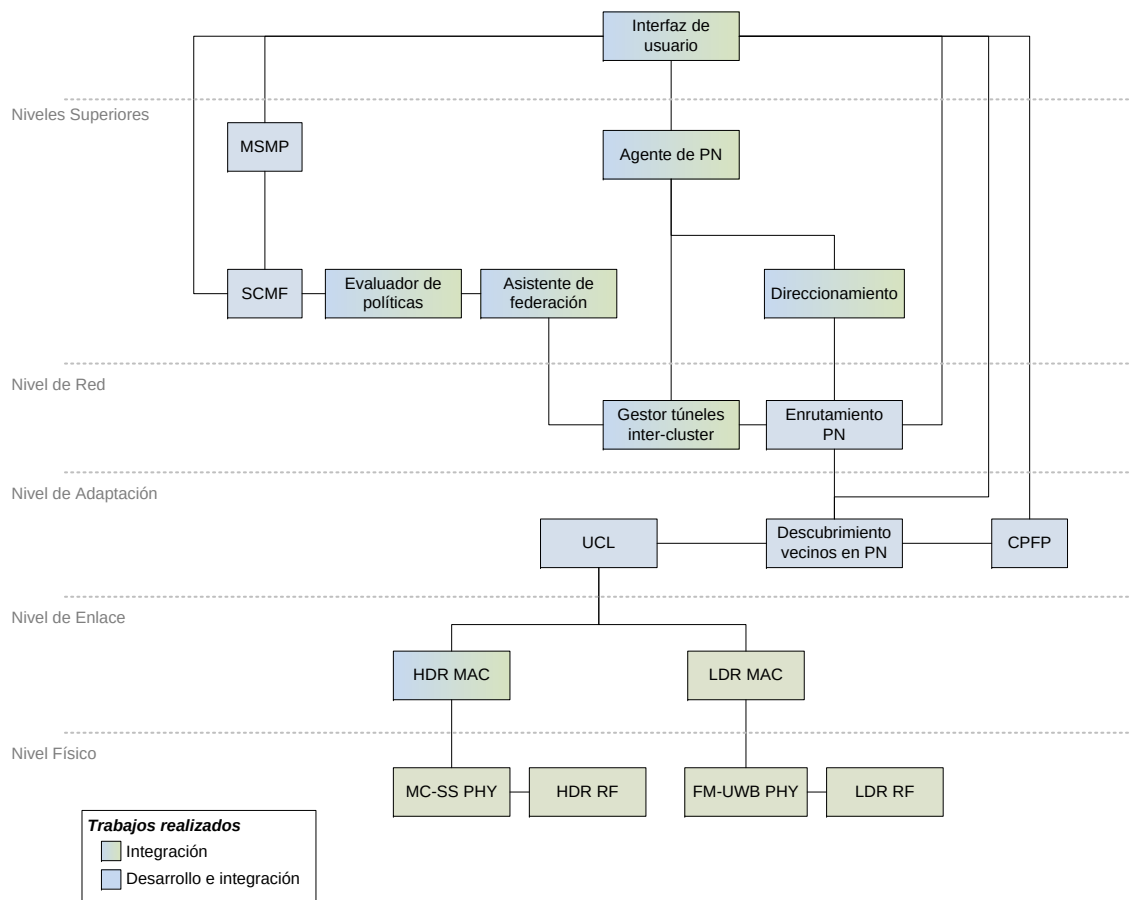


Figura 6.2: Diagrama de bloques de un nodo personal y su PN

Este capítulo describe los trabajos realizados en el desarrollo e integración de los componentes especificados en capítulos anteriores dentro de la plataforma de una PN y PN-F. Como se ve en la figura 6.2, gran parte de los componentes que conforman un nodo personal están vinculados entre sí e incluso con bloques ejecutados en otras máquinas. En este diagrama se han destacado con diferentes colores los trabajos desempeñados en cada uno de los bloques funcionales. Los esfuerzos se centraron fundamentalmente en los componentes de comunicaciones, habilitando soluciones que las hicieran más seguras y dieran soporte a la movilidad, al tiempo que proporcionasen los medios para lograr el acceso a la información

estadística de los canales inalámbricos y el entorno de los nodos de usuario en forma de datos de contexto.

Por otro lado, es importante señalar que las soluciones planteadas para dar respuesta a la arquitectura de una PN y una PN-F, a pesar de ser abiertas e implementables en entornos reales, como se comprobó con el éxito de los proyectos MAGNET y MAGNET Beyond, dependían de la adopción por parte de la comunidad (proveedores, científicos, etc.) para llegar a introducirse en la vida cotidiana de los usuarios. En este sentido, los conceptos y planteamientos detrás de la idea de una red personal sí han sido adaptados años más tarde, pero algunos de los mecanismos y protocolos para implementarlos no han arraigado.

Es por esto que, como complemento al trabajo de validación de las redes personales, se ha considerado necesaria la adaptación de algunas de las soluciones a entornos más comunes y cercanos al usuario, de forma que su aplicación sea más directa. En este sentido, sin abandonar la filosofía de la PN y la PN-F, se han extendido parte de los mecanismos y protocolos sobre soluciones estándares.

Seguidamente se detallan parte de los desarrollos y las adaptaciones incluidas en algunos de los procedimientos. La explicación se realizará siguiendo el orden establecido por el ciclo de vida de la PN y la PN-F. Así, en primer lugar, pues es la base del despliegue de una PN, se describe el proceso de certificación de la PNCA sustentado en el PNDS y las adaptaciones sugeridas para dotarlo de una mayor robustez. A continuación, como paso siguiente una vez que los nodos se consideran personales, se desglosa la implementación de la UCL como habilitadora de la comunicación segura y heterogénea dentro de la PN. Posteriormente, y dada la importancia que en una PN tiene el contexto, se describe el proceso de elección del gestor dentro de los *clusters* basado en las métricas contextuales disponibles. Por último, se lleva a cabo el análisis, adaptación a la PN y validación del despliegue de una solución de movilidad alternativa a la ya implementada en las demostraciones de la PN dentro de los proyectos MAGNET y MAGNET Beyond.

6.1. Certificación de la PNCA

La PNCA se erige como el elemento que junto con el usuario garantiza la identidad de los dispositivos y nodos incluidos en una PN. La propia PNCA es validada por el usuario durante su creación y actúa como CA raíz de la PN, siendo su certificado autofirmado durante el proceso de generación [150, 184].

Esta implementación de la PNCA da soporte a una PN, pero no habilita la posible interacción de dicha PN con otras para conformar PN-F. Se necesita por tanto extender la validez como CA más allá del rango de una PN. La figura del PNDS, analizada en el apartado 5.3.1.1, se plantea como una CA de nivel superior capaz de validar la identidad de una PN y firmar el certificado raíz de ésta, lo que garantizaría la cadena de confianza entre PN.

Siendo rigurosos y siguiendo los procesos establecidos por una PKI para la emisión de certificados personales, el propio usuario debería personarse ante la entidad de confianza para que validando in situ sus datos se diera el visto bueno a la información identificativa que se desea incluir en el certificado. Sin embargo, este modo de operación resta atractivo

a la PN por lo que hay que buscar soluciones que, aunque no integren la seguridad al más alto nivel, sean más cercanas al usuario y estimulen su uso.

En el proyecto MAGNET se planteó el caso de uso en el que los usuarios autentican al PNDS basándose en la información incluida en su certificado, normalmente preinstalado en sus terminales, mientras que el PNDS valida la identidad del usuario mediante la dupla formada por un nombre de usuario, usualmente el número de teléfono, y una clave remitida a su dispositivo, en este caso a través de un *Short Message Service* (SMS). Si bien no es la opción más segura, se considera que el usuario es el único portador de su terminal móvil y por tanto el único que tendrá acceso a la clave remitida. A partir de ese momento, esta dupla será remitida como autenticador de las peticiones que se envíen al PNDS, es decir, solicitud de certificación de la PNCA, petición de registro y búsqueda de PN-F, etc.

En las pruebas piloto realizadas inicialmente, se emplearon como dispositivos de usuario tabletas de Nokia y ordenadores portátiles, alojando la PNCA de forma local. Por extensión, simplemente con trasladar los ficheros de un terminal a otro, cualquier dispositivo con capacidades de cómputo suficientes podría ejercer de PNCA. Sin embargo, operando de esta forma, se permite que cualquiera que tenga acceso al terminal tenga acceso a la clave privada e incluso las claves podrían llegar a estar distribuidas en múltiples nodos, no sabiendo quién es el que realmente juega el rol de PNCA y teniendo información no actualizada.

A lo largo de esta tesis se ha postulado que las tarjetas inteligentes son uno de los emplazamientos más adecuados para alojar las funcionalidades de la PNCA. Las tarjetas inteligentes desde de su concepción se plantearon como dispositivos portables de almacenamiento que incorporan importantes mecanismos de seguridad física, además de criptoprocesadores capaces de ejecutar los algoritmos más actuales. De entre todas, la única tarjeta inteligente que está alojada en terminales con capacidades de comunicaciones es la SIM, incluida en prácticamente la totalidad de los teléfonos móviles.

Incorporar la PNCA en una tarjeta SIM permite definir un elemento exclusivo facultado para soportar la seguridad de la PN. Gracias a las capacidades criptográficas de la SIM, las claves se generarían dentro de la tarjeta y la clave privada no abandonaría nunca el soporte e incluso sería desconocida para el dueño de la PN. Todo ello redundaría en una mayor seguridad.

A continuación, tras introducir la arquitectura *software* del PNDS y la forma en la que éste opera, se describe la implementación del proceso de certificación de la PNCA modificado, donde no sólo la tarjeta SIM genera las claves, sino que implementa los mecanismos necesarios para soportar la autenticación mutua entre el PNDS y la PNCA.

6.1.1. Arquitectura *software* del PNDS

En la figura 6.3 se ilustra la implementación del PNDS realizada. Siguiendo el paradigma de ejecución de aplicaciones remotas, el PNDS despliega una API basada en llamadas *XML-Remote Procedure Call* (RPC) aseguradas mediante SSL que permite acceder a las funcionalidades más relevantes:

- Validar la identidad de la PN.
- Restablecer la clave de acceso.

- Generar el certificado de la PNCA.
- Unirse a la PN-F.

Adicionalmente incluye una base de datos donde se almacenan los registros de las PN y los perfiles de las PN-F.

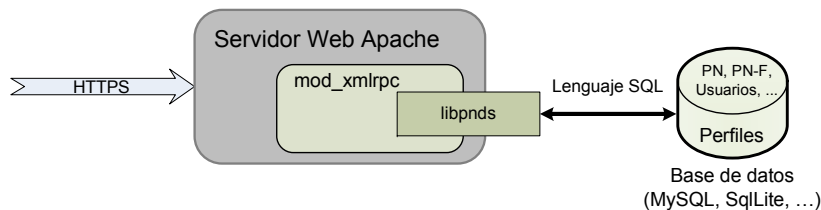
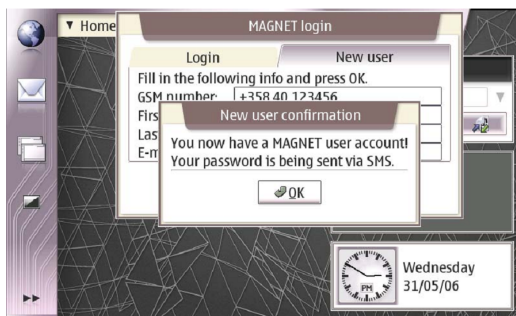


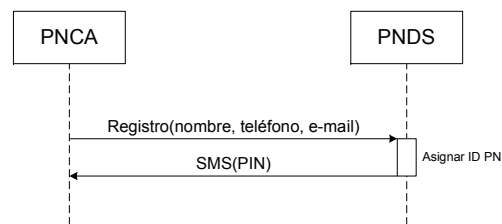
Figura 6.3: Estructura *software* del PNDS

6.1.2. Procedimiento de certificación en MAGNET

El certificado emitido por el PNDS vincula la identidad de la PN a la clave pública de ésta, generada a través de la PNCA. Por lo tanto, lo primero que tiene que realizar un usuario antes de que el PNDS emita la certificación es registrarse para proporcionar la información relativa a su identidad. Haciendo uso de una interfaz gráfica, el usuario remite la petición de registro, creándose una nueva cuenta en la base de datos del PNDS. El identificador asociado inicialmente debe ser el número de teléfono (figura 6.4). El usuario a posteriori puede modificar su perfil e incluir un nombre común para la PN. Como resultado de estas operaciones, el PNDS asigna un prefijo no duplicado a la PN. El resto de los nodos podrán recuperarlo de la PNCA o conectándose al PNDS previa autenticación.



(a) Captura de pantalla



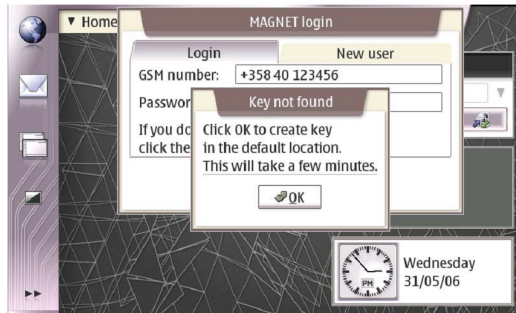
(b) Diagrama de flujo

Figura 6.4: Interfaz de creación de cuenta sobre tableta

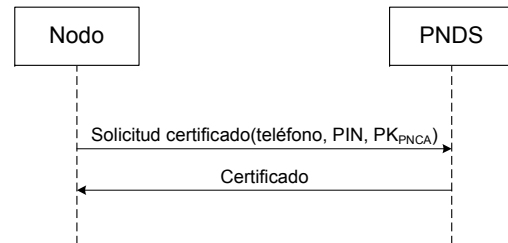
El PNDS genera una clave aleatoria y la asocia a la cuenta recién creada. Esta clave se envía a través de un SMS. Se considera que, puesto que el número de teléfono está asociado a una única persona, ésta es una manera razonable de autenticar al usuario.

A partir de este momento cualquier otra comunicación o consulta que se realice contra el PNDS requiere el identificador del usuario usado y la clave obtenida para validar la

operación. Adicionalmente, la transferencia de datos irá cifrada empleando una sesión SSL segura generada a partir del certificado del PNDS. Para facilitar el funcionamiento se solicita al usuario que realice un acceso autenticado o *login*, emulando de esta manera un sistema *Single Sign On* (SSO).



(a) Captura de pantalla



(b) Diagrama de flujo

Figura 6.5: Proceso de certificación sobre tableta

En la figura 6.5 se muestra el proceso de descarga del certificado del PNDS.

6.1.3. Procedimiento de certificación modificado

Los procesos de identificación recurren a datos que el usuario sabe (número secreto, etc.), a elementos que dicho usuario porta (tarjeta identificadora o memoria USB) y aspectos propios del usuario (p. ej. biometría). Adicionalmente, para dotar de mayor robustez se trata de incluir la mayor variabilidad entre los intentos de autenticación para evitar ataques como la replicación, etc.

El proceso de autenticación e identificación presentado anteriormente se puede considerar, en un sentido estricto, como débil, ya que, además de basar toda la validación en una clave sencilla, el canal por el que el usuario la recibe y por el que se realiza la posterior autenticación no tienen por qué estar vinculados. Es más, es imposible impedir que un usuario registre su PNCA empleando un nodo que no es suyo, es decir, podría recibir su clave de acceso en su terminal móvil y más tarde, tras iniciar la PNCA en un nodo de un amigo, copiar los ficheros de clave y trasladarlos a su propio nodo. En este escenario el usuario asume la responsabilidad de todo el riesgo que toma.

La modificación que se plantea consiste en emplear la tarjeta SIM como elemento de apoyo en el procedimiento de validación y como almacén seguro de las claves de la PNCA. De esta forma se eliminarán los dos riesgos anteriormente reseñados, ya que las claves y el certificado residirán en un mismo soporte durante toda la vida útil de la PN y además se vincularán los canales de autenticación y recepción de información centralizándolos en la propia SIM.

Las tarjetas SIM actuales incorporan un sistema operativo (Java Card™) que permite ejecutar aplicaciones que invoquen procesos de comunicación tanto con el terminal móvil como con la plataforma del proveedor de telefonía móvil a través de protocolos estándar,

Cuadro de texto 6.1: Registro de eventos SAT

```
ToolkitRegistry reg;

.....

// Get a Registry object reference
reg = ToolkitRegistry.getEntry();
// Set the 'Formatted SMS PP Envelope Data Download' event registration
reg.setEvent(EVENT_PROFILE_DOWNLOAD);
reg.setEvent(EVENT_FORMATTED_SMS_PP_ENV);

.....
```

así como operaciones criptográficas. En [194-196] se realiza una descripción de la tecnología de tarjeta inteligente en la que se basan las tarjetas SIM empleadas en la implementación.

Haciendo uso de estas capacidades, a continuación se detalla el diseño y desarrollo del protocolo sobre tarjetas SIM y se describe funcionalmente su operativa. Señalar que se implantó una adaptación de este procedimiento, enfocada a la autenticación genérica en portales web, sobre la plataforma comercial del operador de telefonía móvil Amena, actual Orange, quien proporcionó acceso a sus plataformas de gestión y programación *Over-the-Air* (OTA). Esta colaboración derivó en una petición conjunta de patente del procedimiento desarrollado, que desafortunadamente fue denegada.

6.1.3.1. Descripción funcional

En el momento de adquirir la tarjeta SIM que alojará la PNCA, un delegado del proveedor del servicio (p. ej. el operador de telefonía móvil) valida visualmente la identidad del usuario y personaliza la tarjeta con un conjunto de claves y procedimientos que se usarán durante el proceso de autenticación.

Llegado el momento en que el usuario quiera iniciar su PN y por tanto su PNCA, éste sólo tendrá que acceder a una de las opciones incluidas en el menú *SIM Application Toolkit* (SAT) de su tarjeta, lo que activada el intercambio de mensajes GSM 03.48 [197, 198] con la plataforma OTA del proveedor. El proceso también se podrá iniciar al acceder al servicio remoto a través de Internet.

Aquel servicio que requiera autenticar al usuario, en este caso el PNDS, envía un mensaje a la aplicación de autenticación residente en la tarjeta, pidiendo la comprobación de la identidad del usuario. Puesto que la tarjeta SIM podría alojar varias claves de autenticación asociadas a diferentes servicios, el mensaje enviado indica la clave a utilizar (a través del índice de ésta), un texto que aparecerá como explicación de la acción que se está realizando, y la información a firmar.

El mensaje enviado y que se recibe en la tarjeta SIM se encuentra encapsulado en un mensaje GSM 03.48. A la recepción de dicho mensaje, el terminal móvil comprueba que el *Toolkit Application Reference* (TAR) incluido en el mensaje coincida con alguna aplicación SAT registrada para recibir eventos de tipo *SMS Point-to-Point Data*. En tal caso, dicha aplicación es despertada mediante un comando ENVELOPE que incluye el mensaje recibido (cuadro de texto 6.1).

Una vez que el mensaje se ha enviado a la aplicación SAT residente en la tarjeta, tras

comprobar la integridad de los datos recibidos y su correspondencia con el protocolo empleado, se desencapsula la información. Como se ha comentado, en el propio mensaje se incluye información relativa al servicio sobre el que se desea autenticar. Esta información se presenta en la pantalla del móvil mediante el comando proactivo `DISPLAY TEXT`. En la figura 6.6a se muestra un ejemplo.

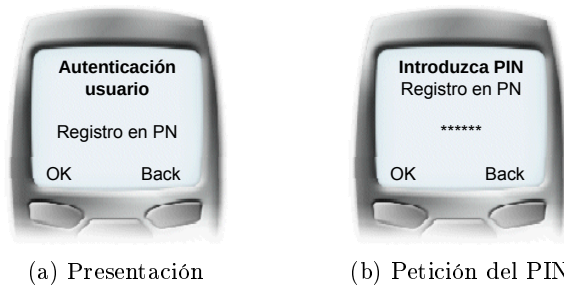


Figura 6.6: Pantallas de inicio del proceso de firma

Al expirar el tiempo de espera o bien al pulsar el usuario sobre la opción OK, se pide el PIN asociado a la clave indicada en el mensaje, tal como se observa en la figura 6.6b. El usuario lo introducirá a través del teclado, siendo recogido por la aplicación mediante un comando `GET INPUT`. Dicho comando `GET INPUT` se codifica de forma que el terminal no muestre la información que introduce el usuario. La aplicación SAT recoge este PIN y si coincide con el asociado a la clave indicada en el mensaje, la desbloquea y cifra los datos enviados según el algoritmo establecido. En caso de que la comprobación del PIN no sea satisfactoria, el usuario puede reintentarlo tantas veces como se haya definido. Una vez que se superen el número máximo de reintentos debe ponerse en contacto con el proveedor de servicios para que proceda a desbloquear el uso de la clave.

Finalmente, tras enviar la respuesta al servidor, se muestra un mensaje al usuario señalando que la acción de autenticación se está llevando a cabo. Si la autenticación mutua resulta positiva, se puede continuar con el procedimiento de descarga del certificado de la PNCA.

Dado que en el momento de la adquisición de la tarjeta SIM, el usuario ya vinculó su número de teléfono y el identificador del chip de la tarjeta (ICCID, *Integrated Circuit Card Identifier*) de la misma, el servidor PNDS puede rellenar los campos personales del certificado sin necesidad de pedírselos al usuario. Únicamente falta la clave pública que asociar para poder finalizar la creación del certificado.

La aplicación residente en la SIM generará automáticamente las claves pública y privada de la PNCA, y mediante otro mensaje GSM 03.48 remitirá la clave pública al PNDS. Se puede observar que la clave privada nunca abandona el dispositivo seguro y que incluso el propio usuario no tiene acceso a ella. Para poder usarla deberá desbloquearla mediante un PIN.

Toda vez que el PNDS genera el certificado, lo remite vía OTA a la aplicación de PNCA en la SIM para que el usuario pueda personalizar sus nodos.

El flujo de mensajes descrito se resume en la figura 6.7.

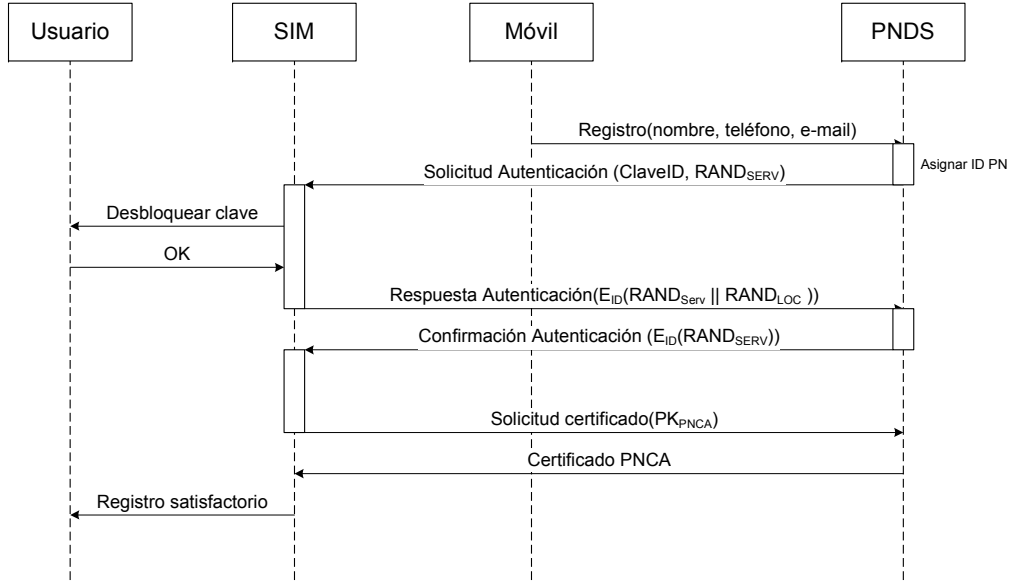


Figura 6.7: Protocolo de validación de identidad modificado

6.1.3.2. Estructura de datos

La aplicación desarrollada gestiona hasta 5 claves de usuario y una clave maestra K_m , utilizada para cambiar las demás claves. La información almacenada asociada a cada clave de usuario se describe en la tabla 6.1. Cada clave tiene asociado un PIN de desbloqueo o uso de longitud variable, que el usuario conoce y puede modificar en cualquier momento. Dado que cada clave se destina a un uso concreto, se incluye un texto explicativo que se presentará, en caso de ser requerido, en la interfaz de usuario de la aplicación. Además, se tienen en cuenta los diferentes requerimientos de seguridad de la aplicación destino a través de la definición de diferentes algoritmos de cifrado para la firma.

La clave maestra K_m tiene una longitud fija de 24 *bytes* y se emplea con el algoritmo criptográfico Triple Data Encryption Standard (3DES), basado en tres iteraciones del algoritmo *Data Encryption Standard* (DES) [199].

Como se ha podido observar hasta ahora, los algoritmos que se emplean para el cifrado de la información se enmarcan dentro de los denominados algoritmos de clave simétrica. Según este modelo, ambos extremos de la comunicación comparten un secreto único que habilita el entendimiento entre ambos. La razón de su utilización en lugar de algoritmos de criptografía asimétrica, que proporcionan una mayor robustez, se debe únicamente a que ofrecen una mayor velocidad en las operaciones y su integración con las plataformas OTA es más sencilla; de ahí su empleo en este sistema de autenticación, más orientado a la validación conceptual. Sin embargo, es importante señalar que la migración a algoritmos de clave asimétrica es prácticamente inmediata, pues sólo se requieren pequeñas modificaciones en el código desarrollado y la mayoría de las tarjetas inteligentes incorporan procesadores criptográficos capaces de operar con estos algoritmos.

Para el almacenamiento del PIN, se emplean 10 *bytes* distribuidos según se presenta en la figura 6.8. El *byte* de control contiene información sobre el número de intentos máximos,

Tabla 6.1: Estructura de datos de la aplicación de autenticación

Campo	Tamaño	Descripción
Índice	1 <i>byte</i>	Identificador de la clave.
Texto	15 <i>bytes</i>	Texto identificativo de la aplicación a la que están asociados la clave y el PIN. Está almacenado en formato Longitud Valor (LV).
PIN	10 <i>bytes</i>	PIN asociado a la clave. El usuario tiene que introducirlo para realizar una autenticación. Se almacena en formato LV, además de un <i>byte</i> de control.
Clave	8, 16, 24 <i>bytes</i>	Valor de la clave. La longitud varía dependiendo del algoritmo usado.
Algoritmo	1 <i>byte</i>	Indica qué algoritmo se usa en las operaciones criptográficas. El valor de este campo puede ser: ■ 00: Ninguno, sólo se realiza la comprobación del PIN. ■ 01: DES. ■ 02: 3DES con 2 claves. ■ 03: 3DES con 3 claves.

el estado de la clave y el número de intentos actuales. Esta distribución busca una forma óptima de almacenamiento que permita el mínimo gasto de memoria en la tarjeta.

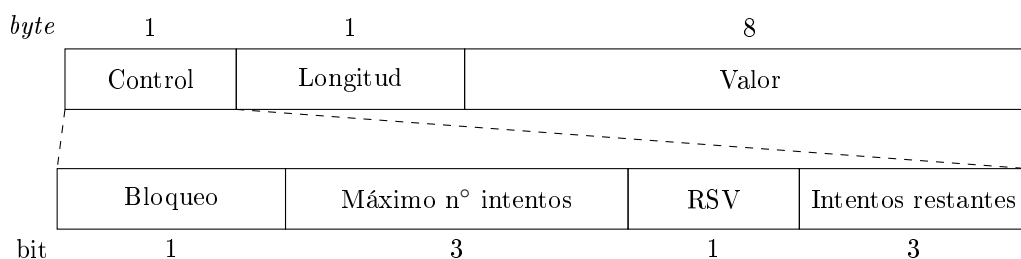


Figura 6.8: Formato del campo PIN

Puede parecer extraño que una plataforma como SAT, orientada al desarrollo de aplicaciones sobre una plataforma de seguridad como es una tarjeta inteligente, no disponga de un sistema de gestión de claves secretas. Esta afirmación es errónea, pues en realidad sí dispone de ella. Sin embargo, el API de seguridad SAT sólo permite la gestión de un PIN por aplicación. Dados los requerimientos funcionales de nuestro sistema, según los cuales se debe disponer de varios números secretos, se hace inviable su empleo y por eso se procede al diseño de una interfaz nueva que se ajuste a las nuevas funcionalidades.

6.1.3.3. Interfaz de gestión local

Además de almacenar la información anteriormente descrita, se desarrolla una interfaz de usuario que permita su modificación, dotando así de una funcionalidad completa al sistema. Para ello se crea un menú a través del cual, de manera local y en cualquier momento, el usuario puede personalizar los números secretos (figura 6.9). Dicho menú aparece como una entrada en el menú SAT con un título a definir en la instalación de la aplicación. Al ejecutarlo se despliega una pantalla de selección con 5 opciones, implementada mediante un comando `SELECT ITEM`, a través de las cuales se modifica el PIN asociado a una clave. El mensaje para cada opción se corresponde con el texto asociado a las distintas claves. El usuario elige el PIN que quiere modificar, y la aplicación le pide, mediante varios comandos `GET INPUT`, el PIN antiguo y el PIN nuevo (2 veces). La aplicación comprueba si el PIN es correcto y actualiza su valor. En el cuadro de texto 6.2 se detalla el código Java Card empleado en la implementación.



Figura 6.9: Pantalla de la interfaz de gestión del PIN

La gestión de las claves (personalización, actualización, bloqueo, etc.) así como su uso (requerimientos de firma, etc.) corre a cargo del operador o proveedor del servicio, por lo se implementa una interfaz que habilite su gestión de manera remota a través de mensajes GSM 03.48, tal como se describe a continuación. No obstante, la aplicación incorpora también una interfaz local de gestión a través de comandos *Application Protocol Data Unit* (APDU) que replica el comportamiento remoto, algo de mucha utilidad durante las fases de puesta en marcha y que se emplearon además durante la fase de desarrollo.

6.1.3.4. Protocolo de intercambio remoto

A partir de la descripción funcional realizada, se extraen las necesidades en cuanto al conjunto de mensajes que se intercambian entre la aplicación SAT y el servidor remoto. Seguidamente se describe la estructura de estos mensajes, incluidos en la figura 6.7, que será replicada en la implementación realizada. Estos mensajes, como se ha insistido anteriormente, se encapsulan sobre mensajes GSM 03.48 y su estructura podría modificarse de forma sencilla para adaptarse a otros requisitos de seguridad más allá de la PN, como puede ser el acceso seguro a cualquier entorno web.

El protocolo implementado se basa en el paradigma comando-respuesta, si bien haciendo uso de las cabeceras *Security Parameters Indication* (SPI) en los mensajes GSM 03.48 se puede instar a no remitir la respuesta o remitirla solo en caso de error para disminuir el

Cuadro de texto 6.2: Cambio de PIN

```

private void changePIN()
{
    short i;
    short sUserKeyRecord;

    ProactiveHandler proHdlr = ProactiveHandler.getTheHandler();
    ProactiveResponseHandler respHdlr = ProactiveResponseHandler.getTheHandler();

    proHdlr.init(PRO_CMD_SELECT_ITEM, (byte)0x00, DEV_ID_ME);
    for (i = 0; i < NUM_RECORDS_TABLE_KEYS; i++) {
        sUserKeyRecord = (short)((i * KEY_RECORD_LENGTH) + KEY_TEXT);
        proHdlr.appendTLV((byte)(TAG_ITEM | TAG_SET_CR), (byte)i,
            m_rgbUserKeysTable, (short)(sUserKeyRecord + 1),
            (short)m_rgbUserKeysTable[sUserKeyRecord]);
    }
    i = proHdlr.send();
    if (i > (byte)9) {
        return;
    }

    // Get the item selected
    i = respHdlr.getItemIdentifier();
    sUserKeyRecord = (short)(i * KEY_RECORD_LENGTH);

    // Check if PIN is blocked
    if ((this.m_rgbUserKeysTable[(short)(sUserKeyRecord + KEY_PIN_CONTROL)] &
        KEY_PIN_BLOCK) == KEY_PIN_BLOCK) {
        // Type : TEXT content : PIN bloqueado
        // coding : 8 bits record : 0x4F (0x2D+0x21+0x01)
        proHdlr.initDisplayText((byte)0x00, DCS_8_BIT_DATA, TEXT, (short)(0x4F+0x01),
            TEXT[(short)0x4F]);
        // Send the built command
        proHdlr.send();
        return;
    }

    if (getAndCheckPIN(sUserKeyRecord, CHANGE_PIN, (short)0) != GET_PIN_OK) {
        return;
    }

    do {
        // Type : TEXT content : Código PIN nuevo
        // coding : 8 bits record : 0x13 (0x00+0x12+0x01)
        if ((i = getNumberPIN(m_rgbPIN, (short)0, CHANGE_PIN, (short)0x13)) ==
            GET_PIN_COMMAND_ERROR) {
            return;
        }
    } while (i == GET_PIN_NUMBER_ERROR);

    do {
        // Type : TEXT content : Confirmar código
        // coding : 8 bits record : 0x25 (0x13+0x11+0x01)
        if ((i = getNumberPIN(m_rgbTemp, (short)0, CHANGE_PIN, (short)0x25)) ==
            GET_PIN_COMMAND_ERROR) {
            return;
        }
    } while (i == GET_PIN_NUMBER_ERROR);

    if (Util.arrayCompare(m_rgbTemp, (short)0, m_rgbPIN, (short)0, (short)(m_rgbPIN[0] +
        1)) != (byte)0x00) {
        // Type : TEXT content : PIN incorrecto
        // coding : 8 bits record : 0x2D (0x00+0x12+0x01)
        proHdlr.initDisplayText((byte)0x00, DCS_8_BIT_DATA, TEXT, (short)(0x2D+1),
            (short)14);
        proHdlr.send();
    } else {
        Util.arrayCopy(m_rgbPIN, (short)0, this.m_rgbUserKeysTable,
            (short)(sUserKeyRecord + KEY_PIN_VALUE),
            (short)(m_rgbPIN[0] + 1));
        // Type : TEXT content : Código PIN cambiado
        // coding : 8 bits record : 0x37 (0x25+0x11+0x01)
        proHdlr.initDisplayText((byte)0x00, DCS_8_BIT_DATA, CHANGE_PIN, (short)(0x37+1),
            CHANGE_PIN[(short)0x37]);
        proHdlr.send();
    }
}

```

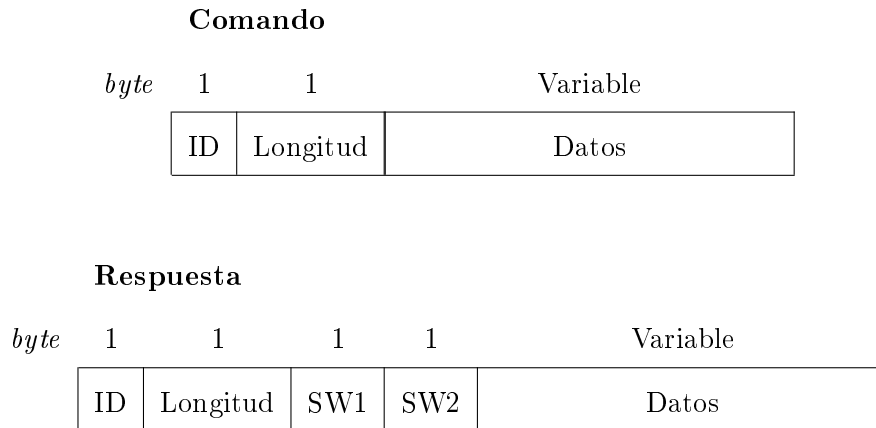


Figura 6.10: Estructura de los comandos y respuestas empleados para la autenticación

volumen de mensajes. El formato de los comandos y las respuestas se puede observar en la figura 6.10; tratan de mantener una estructura muy similar a las APDU International Organization for Standardization (ISO) 7816 de comandos y respuestas [200]. El campo Longitud representa la longitud del campo Datos en *bytes*, mientras que las respuestas incluyen dos *bytes* de estado (SW, *Status Word*), SW1 y SW2, que indican el resultado de la ejecución del comando.

6.1.3.4.1. Secuencia de autenticación

Se describe a continuación la secuencia de mensajes que se emplea para que la tarjeta SIM y el servidor validen sus respectivas identidades.

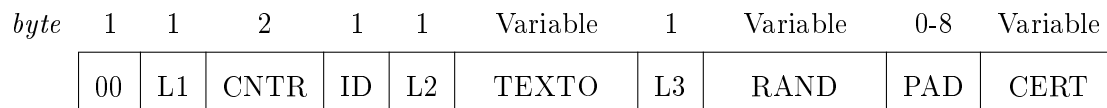


Figura 6.11: Estructura del comando “Envío de reto de autenticación”

El primer mensaje remitido lo envía el servidor remoto, que quiere validar la identidad del usuario, y su formato se representa en la figura 6.11 donde

- **L1** indica la longitud de todos los campos restantes (sin incluir el mismo).
- **CNTR** es un contador que indica el número de comando que se ha enviado. De esta manera se tiene una asociación entre el RAND y el comando en el servidor.
- **ID** indica con qué clave se debe hacer la firma.
- **L2** es la longitud del campo TEXTO en *bytes*.
- **TEXTO** es el texto que se muestra como indicación para la firma. Su longitud máxima es de 100 caracteres.

- **L3** es la longitud en *bytes* del campo **RAND**.
- **RAND** son los datos que se tienen que firmar.
- **PAD** es un campo de relleno. Su longitud es la mínima para conseguir que la longitud desde **CNTR** hasta **PAD** (ambos incluidos) sea múltiplo de 8.
- **CERT** es el certificado resultante de realizar un 3DES *Cyclic Block Ciphering* (CBC) a los campos anteriores desde **ID** hasta **PAD** (ambos incluidos) con los primeros 8 bytes de la clave maestra K_m .

A este primer mensaje se responde con el mensaje de la figura 6.12 donde

- **L1** indica la longitud de todos los campos restantes (sin incluirse él mismo).
- **SW1** y **SW2** indican el resultado del comando.
- **CNTR** es un contador identificativo del comando al que corresponde la respuesta.
- **ID** indica con qué clave se ha realizado la firma. Debe tener el mismo valor que el campo **ID** del comando.
- **RAND firmado** es el resultado de cifrar con la clave indicada el campo **RAND** que se envió en el comando concatenado con un **RAND** adicional generado por la tarjeta, que deberá ser devuelto firmado. Si la clave con la que se realiza la firma tiene asociado el algoritmo 0x00, el valor del campo **RAND firmado** se transmite en claro.
- **PAD** es un campo de relleno. Su longitud es la mínima para conseguir que la longitud desde **SW1** hasta **PAD** (ambos incluidos) sea múltiplo de 8.
- **CERT** es el certificado resultante de realizar un 3DES CBC a los campos anteriores desde **SW1** hasta **PAD** (ambos incluidos) con los primeros 8 *bytes* de la clave maestra K_m .

Error en la ejecución

<i>byte</i>	1	1	1	1
	01	L1	SW1	SW2

Ejecución satisfactoria

<i>byte</i>	1	1	1	1	2	1	Variable	0-8	8
	01	L1	90	00	CNTR	ID	$E_{ID}(\text{RAND}_{SERV} \parallel \text{RAND}_{SIM})$	PAD	CERT

Figura 6.12: Estructura del comando “Respuesta ante reto de autenticación”

Por último, el servidor remite la confirmación de autenticación satisfactoria o errónea por su parte, tal como se refleja en la figura 6.13 donde

- **L1** indica la longitud de todos los campos restantes (sin incluirse él mismo).
- **SW1** y **SW2** indican el resultado del comando.
- **CNTR** es un contador identificativo del comando al que corresponde la respuesta.
- **ID** indica con qué clave se ha realizado la firma. Debe tener el mismo valor que el campo ID del comando.
- **RAND firmado** es el resultado de cifrar con la clave indicada el campo RAND que se envió en el comando concatenado con un RAND adicional generado por la tarjeta, que deberá ser devuelto firmado. Si la clave con la que se realiza la firma tiene asociado el algoritmo 0x00, el valor del campo RAND firmado se transmite en claro.
- **PAD** es un campo de relleno. Su longitud es la mínima para conseguir que la longitud desde SW1 hasta PAD (ambos incluidos) sea múltiplo de 8.
- **CERT** es el certificado resultante de realizar un 3DES CBC a los campos anteriores desde SW1 hasta PAD (ambos incluidos) con los primeros 8 *bytes* de la clave maestra K_m .

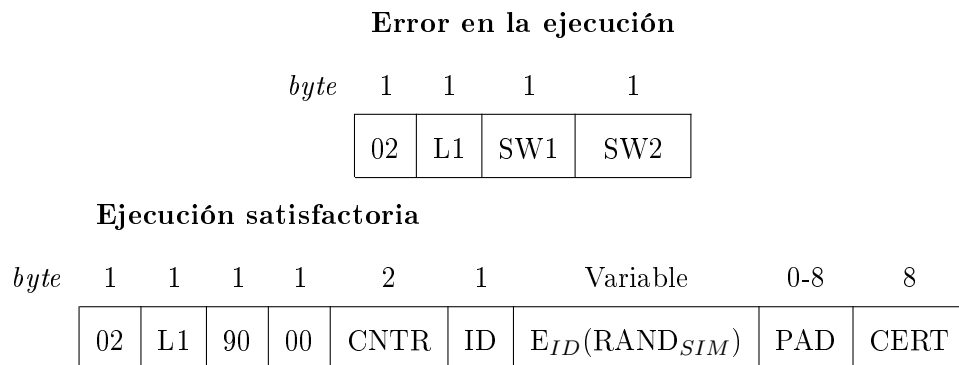


Figura 6.13: Estructura del comando “Envío de confirmación de autenticación”

La validación correcta por parte de la tarjeta del valor retornado por el servidor haría que se procediera a continuar con el procedimiento que se estuviera realizando, en el caso que nos conlleva, la generación del certificado de la PNCA.

6.1.3.4.2. Actualización de clave de usuario o clave maestra

Este comando permite cambiar el valor de alguna clave o de un campo asociado a la misma. Como se ha indicado anteriormente, las claves son desconocidas por el usuario y el operador, quien viendo comprometida su integridad, puede proceder a su actualización o modificación para restaurar la seguridad del sistema. El formato del comando se describe en la figura 6.14 donde

- **L1** indica la longitud de todos los campos restantes (sin incluirse él mismo).

<i>byte</i>	1	1	2	1	1	Variable	1	Variable	1	0-8	8
	04	L1	CNTR	ID	L2	TEXTO	L3	CLAVE	ALG	PAD	CERT

Figura 6.14: Estructura del comando “Cambio de clave”

- **CNTR** es un contador que identifica el comando que se ha enviado. De esta manera se mantiene una relación unívoca en el servidor entre los datos enviados y el comando.
- **ID** indica la clave que va a ser modificada.
 - 0x00 ... 0x04: clave de usuario.
 - 0xFF: clave maestra.
- **L2** es la longitud del campo **TEXTO** en *bytes*.
- **TEXTO** es el texto identificativo asociado a la clave. Su longitud máxima es de 15 caracteres.
- **L3** es la longitud en *bytes* del campo **CLAVE**.
- **CLAVE** es el nuevo valor de la clave.
- **ALG** indica el algoritmo que se utilizará con la clave indicada.
- **PAD** es un campo de relleno. Su longitud es la mínima para conseguir que la longitud desde **ID** hasta **PAD** (ambos incluidos) sea múltiplo de 8.
- **CERT** es el certificado resultante de realizar un 3DES CBC con 3 claves a los campos anteriores, desde **CNTR** hasta **PAD** (ambos incluidos) con la clave maestra K_m .

Dado que este comando requiere una seguridad adicional que garantice la integridad del intercambio, los datos desde **CNTR** hasta **CERT** (ambos incluidos) se cifran con DES CBC utilizando como clave los primeros 8 *bytes* de la clave K_m . Señalar igualmente que, en el caso de realizarse la actualización de la clave maestra, el campo **TEXTO** incluye un valor aleatorio.

La respuesta a este comando presenta el formato de mensaje que se describe en la figura 6.15 donde

- **L1** indica la longitud de todos los campos restantes (sin incluirse él mismo).
- **SW1** y **SW2** indican el resultado del comando.
- **CNTR** es el contador identificativo del comando al que corresponde la respuesta.
- **ID** indica qué clave ha sido modificada. Debe tener el mismo valor que el campo **ID** del comando.

- **TEXTO** es el mismo campo TEXTO enviado en el comando, cifrado con la nueva clave.
- **PAD** es un campo de relleno. Su longitud es la mínima para conseguir que la longitud desde SW1 hasta PAD (ambos incluidos) sea múltiplo de 8.
- **CERT** es el certificado resultante de realizar un 3DES CBC a los campos anteriores desde SW1 hasta PAD (ambos incluidos) con los primeros 8 *bytes* de la clave maestra K_m .

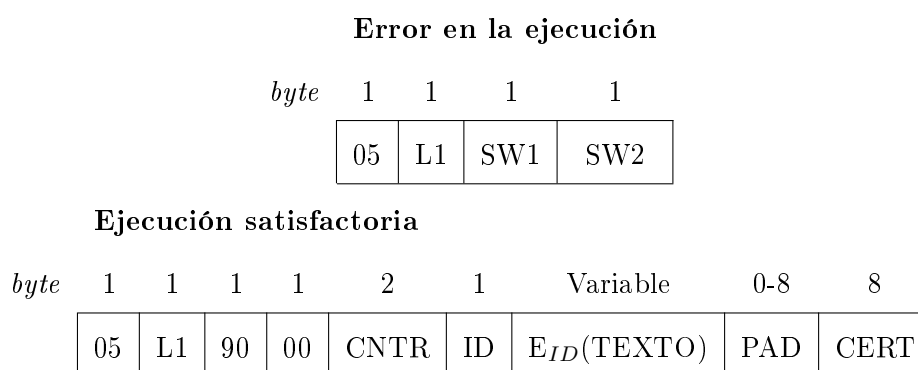


Figura 6.15: Estructura de la respuesta “Cambio de clave”

Cabe indicar que los datos desde SW1 hasta CERT (ambos incluidos) están cifrados con DES CBC utilizando como clave los primeros 8 *bytes* de la clave K_m . En el caso de que se realice la modificación de la clave maestra, el cálculo del certificado y del cifrado se lleva a cabo con el valor antiguo de la clave. Si todos los pasos se ejecutan satisfactoriamente, a partir del próximo comando se utilizará el nuevo valor de la clave maestra.

6.1.3.4.3. Desbloqueo de clave

Está demostrado que un usuario es propenso a perder o no recordar su clave de acceso al sistema. En la mayoría de los casos, a pesar de desconocerlo, el usuario intenta introducir su clave o PIN de nuevo, llegando en muchos casos a bloquear la tarjeta o aplicación. Es por esto que se hace necesario, no sólo para facilitar la tarea al operador sino también para dotar de un valor añadido al usuario, que la aplicación desarrollada incluya un procedimiento de desbloqueo, mediante el cual se restaure el número máximo de intentos permitidos para el PIN asociado a una clave.

El formato del comando se describe en la figura 6.16 donde

- **L1** indica la longitud de todos los campos restantes (sin incluirse él mismo).
- **CNTR** es un contador que asocia unívocamente el RAND enviado y el comando en el servidor.
- **ID** indica la clave asociada al PIN que se quiere desbloquear.

- **L2** es la longitud del campo PIN en *bytes*.
- **PIN** es un valor del nuevo PIN asociado a la clave. Este PIN podría enviarse cifrado con la clave correspondiente.
- **L3** es la longitud del campo RAND en *bytes*.
- **RAND** es un valor aleatorio que se utiliza para aumentar la seguridad, ya que de esta forma se aleatoriza la cadena enviada.
- **PAD** es un campo de relleno. Su longitud es la mínima para conseguir que la longitud desde ID hasta PAD (ambos incluidos) sea múltiplo de 8.
- **CERT** es el certificado resultante de realizar un 3DES CBC a los campos anteriores desde CNTR hasta PAD (ambos incluidos) con la clave maestra K_m .

<i>byte</i>	1	1	2	1	1	Variable	1	Variable	0-8	8
	06	L1	CNTR	ID	L2	PIN	L3	RAND	PAD	CERT

Figura 6.16: Estructura del comando “Desbloqueo de clave”

Los datos desde CNTR hasta CERT (ambos incluidos) se cifran con DES CBC, utilizando como clave los primeros 8 *bytes* de la clave K_m .

La confirmación de la correcta actualización de la clave se encapsula en una respuesta formateada según lo dispuesto en la figura 6.17 donde

- **L1** indica la longitud de todos los campos restantes (sin incluirse él mismo).
- **SW1** y **SW2** indican el resultado del comando.
- **CNTR** es el contador identificativo del comando al que corresponde la respuesta.
- **ID** indica qué clave está asociada al PIN desbloqueado. Debe tener el mismo valor que el campo ID del comando.
- **RAND** es el mismo campo RAND enviado en el comando.
- **PAD** es un campo de relleno. Su longitud es la mínima para conseguir que la longitud desde SW1 hasta PAD (ambos incluidos) sea múltiplo de 8.
- **CERT** es el certificado resultante de aplicar 3DES CBC a los campos anteriores, desde SW1 hasta PAD (ambos incluidos), con los primeros 8 *bytes* de la clave maestra K_m . En el caso de que se realice la modificación de la clave maestra, el cálculo del certificado y del cifrado se realiza con el valor antiguo de la clave. Si todos los pasos se llevan a cabo satisfactoriamente, a partir del próximo comando se utilizará el nuevo valor de la clave maestra.

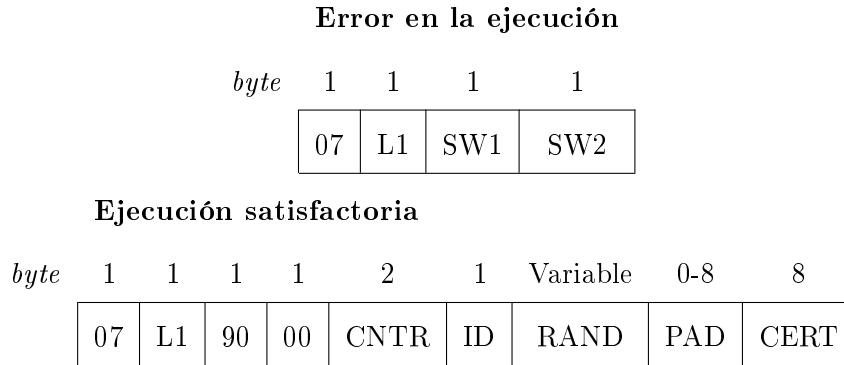


Figura 6.17: Estructura de la respuesta “Desbloqueo de clave”

Como ocurre con la respuesta al comando de actualización de clave, los datos desde SW1 hasta CERT (ambos inclusive) van cifrados con DES CBC utilizando como clave los primeros 8 *bytes* de la clave maestra K_m .

Adicionalmente, dado que los mensajes GSM 03.48 se intercambian de manera transparente para el usuario, toda vez que se recibe la confirmación de la reactivación de la clave, se le remite un SMS al usuario con el nuevo PIN, de forma que pueda hacer uso de dicha clave.

6.2. Capa Universal de Convergencia

Establecida la cadena de confianza que soporta el procedimiento CPFPP con el que se personalizan los nodos empleando cualquiera de los métodos anteriormente descritos, éstos ya se encuentran totalmente funcionales para operar dentro de la PN. La PN siempre se ha planteado como una red de comunicaciones heterogénea a nivel de RAT. Cada RAT dispone de su propia metodología de gestión de la seguridad y de las comunicaciones, lo que dificulta la interacción del usuario con sus nodos y, en cierto modo, hace difícil extender la relación de confianza establecida entre ellos.

La UCL se presentó en el apartado 3.4 como un nivel de abstracción dentro de la arquitectura de red de la PN que, haciendo uso de mecanismos de optimización intercapas, permite la gestión inteligente y transparente de las interfaces radio disponibles en los dispositivos y nodos de usuario.

Más allá de la especificación y descripción de su arquitectura de alto nivel, la implementación y posterior validación del concepto de UCL se encuentra como uno de los objetivos destacados de esta tesis y será tratado a continuación.

6.2.1. Arquitectura *software*

Identificada como una capa intermedia entre los niveles de enlace y red de la pila de protocolos estándar, la UCL extiende el concepto de *Performance Enhancing Proxy* (PEP) [201] empleado dentro del ámbito de proyectos como *Wireless Internet Networks* (WINE) [202] o PACWOMAN [42]. Además de incorporar el descubrimiento de nodos personales y el

establecimiento de canales seguros entre ellos, haciendo frente a uno de los requerimientos claves de una PN, permite enmascarar la existencia de múltiples interfaces radio, haciendo así posible la comunicación entre nodos operando en diferentes DR, la optimización de rutas entre ellos e incluso la mejora de la calidad del enlace.

La arquitectura de alto nivel planteada en el diagrama de la figura 3.8 se hace realidad empleando el trabajo combinado entre utilidades ejecutándose en el espacio de usuario e implementaciones en el espacio de *kernel*. Las primeras ofrecen un entorno amigable de gestión y acceso a las funcionalidades y datos que la UCL proporciona. Así, se emplearán durante el proceso de inicialización y las comunicaciones entre procesos, por ejemplo con la SCMF. Por su parte, el espacio de *kernel* se encarga de todas aquellas tareas que requieren de las modificaciones de los flujos de datos entrantes y salientes, tales como cifrar las comunicaciones, variar la interfaz de salida adaptándola al contexto del nodo, etc.

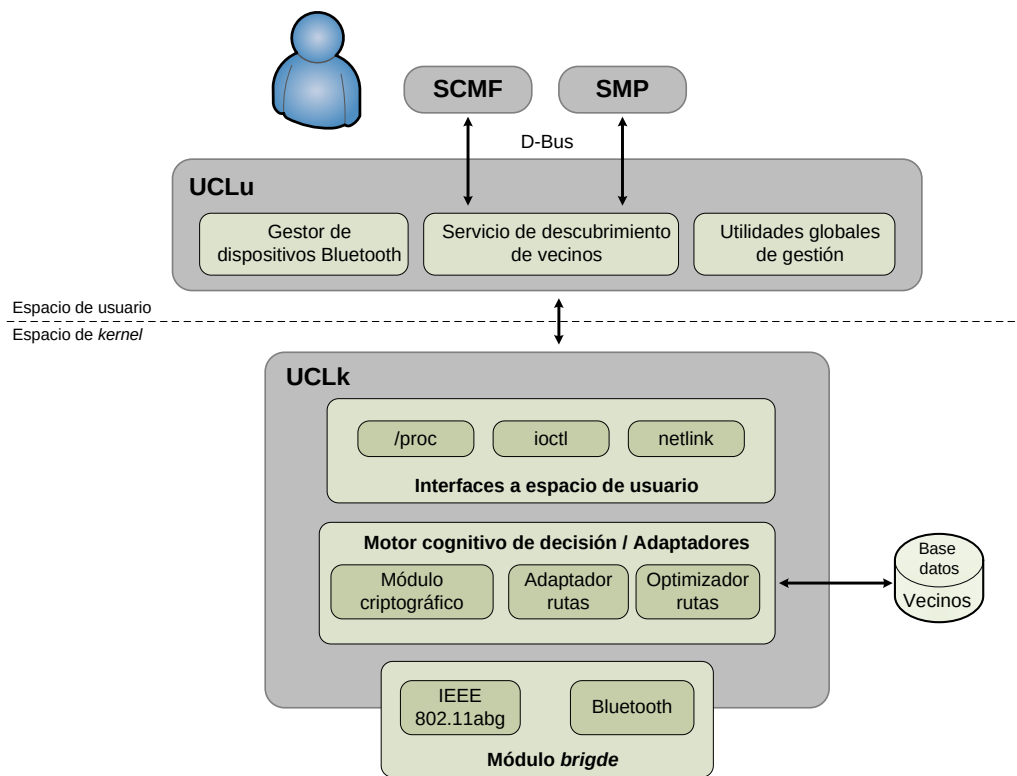


Figura 6.18: Arquitectura *software* de la UCL

El módulo de descubrimiento de nodos vecinos, vital para la operativa de una PN, aunque conceptualmente independiente, gestiona la información que rige el comportamiento de la UCL. Es este módulo el que permite descubrir gran parte de las capacidades de comunicaciones de los nodos personales, como las interfaces disponibles, el estado del canal, etc. Además es el responsable de la negociación del canal seguro de comunicaciones, resultado del que se derivan las claves bilaterales empleadas en el cifrado de las transmisiones entre nodos. Por todo esto, la implementación de la UCL y el módulo de descubrimiento de vecinos se ha llevado a cabo compartiendo interfaces internos y ofreciendo canales de gestión de forma conjunta.

Para el desarrollo de la UCL se ha optado por ocultar todas las interfaces de red existentes en un nodo bajo el paraguas de una única interfaz de red virtual. El concepto de UCL no restringe la implementación en este aspecto, pudiendo haberse decantado por mantener la identidad propia de cada interfaz y ser la UCL quien las gestione. No obstante, la elección realizada favorece la definición de una única dirección identificativa del nodo personal, al tiempo que facilita la labor del módulo de descubrimiento de vecinos.

Una interfaz de red a nivel *software* es un intermediario en el procesamiento de la información dentro de la pila de protocolos que, interactuando con el *driver*, redirige los paquetes recolectados a través del *hardware* subyacente. La UCL, en tanto en cuanto no está ligada a un dispositivo *hardware*, difiere de este concepto y se considera como una interfaz virtual.

Existen diversas formas de implementar este comportamiento en los entornos Linux, plataforma seleccionada para los trabajos de implementación relacionados con la UCL. Soluciones como la *Wireless Adaptation Layer* (WAL) [91, 92], la *PAN and CAN Optimisation Layer* (PCOL) [93] o la más reciente *Generic Link Layer* (GLL) [100], optan por definir un tipo de protocolo Ethernet propio sobre el que se encapsula todo el tráfico de comunicaciones de un nodo. En cierta forma, este identificador de protocolo actúa como una interfaz virtual, ya que la gestión de los paquetes entrantes y salientes se concentra en un único punto. Esta opción no se consideró óptima para la UCL pues, por la configuración de red (tabla de rutas, etc.) que se debe seguir en los nodos que las incorporan, las comunicaciones de un nodo se circunscriben únicamente a aquellos que implementen el mismo tipo de interfaz/protocolo. Esto no es aceptable para la UCL dado que un nodo personal tiene que ser capaz de comunicarse con cualquier nodo externo.

Las opciones más adecuadas en línea con los requerimientos de la UCL pasan por definir un dispositivo de red virtual, lo que se puede conseguir emulando la existencia de una fuente externa empleando soluciones de espacio de usuario como TUN/TAP [203] o diseñando un *driver* de red que, en lugar de estar asociado a un dispositivo físico, se sustente en interfaces que sí lo están para la transmisión y recepción de paquetes. En el momento de emprender el desarrollo de la UCL, TUN/TAP no disponía de una implementación robusta e incurría en un retardo de comunicaciones adicional al tener los paquetes que realizar la transición entre espacio de *kernel* y usuario y viceversa. En consecuencia, se opta por implementar la UCL como un *driver* (dispositivo) de red virtual que procesará los paquetes inyectándolos sobre la interfaz real según las condiciones.

Por definición una interfaz puente (*bridge*) es una interfaz lógica que permite unir varios segmentos de red. La concepción de la UCL busca también servir de base para interconectar varios DR, por lo que tomar la implementación de un *bridge* como base podría ayudar en el desarrollo.

Tras analizar el código fuente del módulo del *kernel* bridge y la librería de control en espacio de usuario *bridge-utils* se comprueba que la estructura y comportamiento implementado se alinea con los requerimientos de la UCL. Es por esto que el esqueleto de la UCL nace como un *bridge* al que se le suprimen todas las funcionalidades de direccionamiento y control incluidas en el protocolo IEEE 802.1d y del que únicamente se mantienen las estructuras para reunir múltiples interfaces.

Sobre este cimientto se añaden las funcionalidades que restan para hacer realidad la ar-

quitectura *software* de la figura 6.18. De una parte se implementa el módulo del *kernel* UCLk como plataforma sobre la que se integran las funcionalidades de la nueva interfaz de red virtual. La capacidades como *pseudo-bridge* permiten al módulo UCLk desempeñar las actividades consideradas para la CdA dentro de la UCL.

La operativa del módulo UCLk analiza los paquetes recibidos y transmitidos en función de la dirección IP y la MAC. Con la primera es capaz de discernir si el nodo emisor o destinatario es un nodo personal, mientras que la dirección MAC permite identificar la interfaz inalámbrica empleada para la transmisión. Para ello la UCL correla la información incluida en el paquete con la adquirida por el módulo de descubrimiento de vecinos que, a partir de mensajes de difusión, ha rellenado una base de datos con información global de la estructura tanto de la PN como de la PN-F (ver figura 6.19).

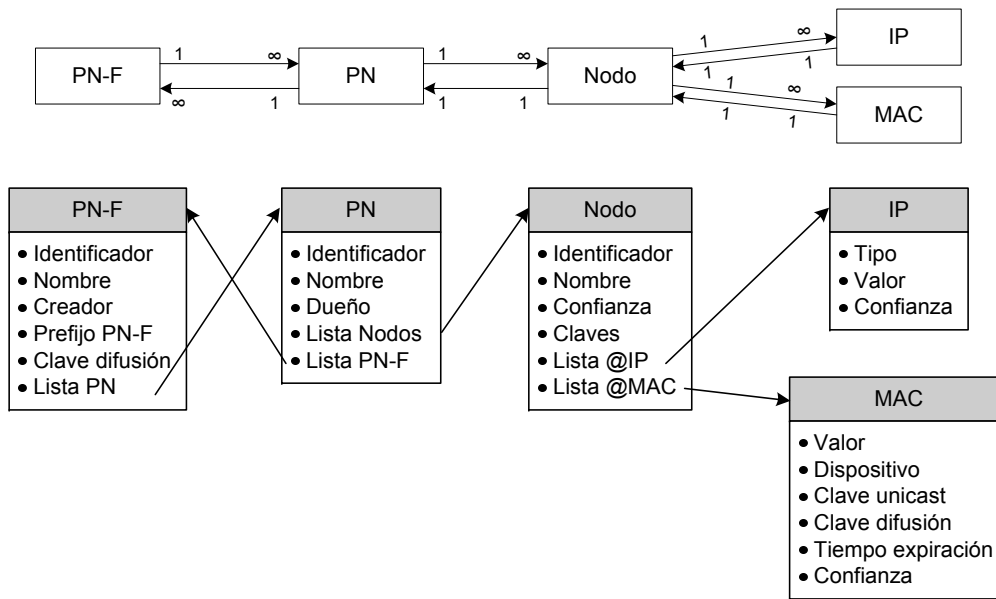


Figura 6.19: Base de datos del módulo de descubrimiento de vecinos

En este sentido, la comunicación con nodos estándares (sin UCL) se sustenta en los mecanismos estándar de resolución de direcciones (*Address Resolution Protocol* (ARP) para IPv4 o descubrimiento de vecinos en IPv6, *Neighbour Discovery* (ND)) para rellenar la cabecera MAC de los paquetes salientes. Dado que la UCL usa una dirección MAC virtual (realmente se corresponde con una de las interfaces bajo su control) puede ocurrir que esta no se corresponda con la interfaz empleada para la comunicación con el nodo estándar. Para prevenir esas situaciones la UCL intercepta los paquetes de resolución de direcciones (ARP o ND) y modifica los campos tanto de cabecera como de datos necesarios de esos paquetes de forma que la información se corresponda con la interfaz a través del cual se establece el canal de comunicación.

El módulo UCLk también incorpora el MCD, como la propia lógica que analiza los paquetes recogidos y remitidos a través del *pseudo-bridge* y sobre los que se aplican las modificaciones definidas por los adaptadores de protocolos desarrollados. Entre éstos destaca

Cuadro de texto 6.3: Creación del dispositivo virtual - Código de UCLk

```
/**
 * Creates and initialized a new UCL device
 *
 * |param name Name of the new UCL device
 *
 * |return Device structure
 */
static struct net_device *new_ucl_dev(const char *name)
{
    struct net_bridge *ucl;
    struct net_device *dev;

    dev = alloc_netdev(sizeof(struct net_bridge), name, ucl_dev_setup);
    if (!dev) {
        return NULL;
    }

    ucl = netdev_priv(dev);
    ucl->dev = dev;

    ...

    return dev;
}

/**
 * Setup device by assinging net_device struct entries
 *
 * |param dev Device to be initilized
 */
void ucl_dev_setup(struct net_device *dev)
{
    DBG_IN();

    memset(dev->dev_addr, 0, ETH_ALEN);

    ether_setup(dev);
    dev->do_ioctl = ucl_dev_ioctl;
    dev->get_stats = ucl_dev_get_stats;
    dev->hard_start_xmit = ucl_dev_xmit;
    dev->open = ucl_dev_open;
    dev->set_multicast_list = ucl_dev_set_multicast_list;
    dev->change_mtu = ucl_change_mtu;
    dev->mtu = 1496;
    dev->destructor = free_netdev;
    SET_MODULE_OWNER(dev);
    dev->stop = ucl_dev_stop;
    dev->tx_queue_len = 0;
    dev->set_mac_address = NULL;
    dev->priv_flags = IFF_EBRIDGE;
}
```

la integración realizada del módulo criptográfico y el optimizador de rutas. En los cuadros de texto 6.3 a 6.6 se pueden observar extractos de código del módulo UCLk.

Además, el módulo UCLk implementa interfaces de intercambio de datos entre el espacio de *kernel* y usuario, de forma que existan rutinas de control habilitadas para su uso en las aplicaciones y servicios de usuario. Existe una gran diversidad de mecanismos en los entornos Linux por lo que, para no limitar las posibilidades de interacción con la UCL, se ha optado por implementar el mayor número de ellos posible. Se han proporcionado interfaces a través de los sistemas de ficheros virtuales `/proc` y `/sys`, del entorno de `ioctl` o mediante *Netlink sockets* [204, 205], siendo la implementación de la captura de datos y la interpretación de los comandos de control común para todos ellos. Como ejemplo, a través de estas interfaces se notifica el descubrimiento de nuevos nodos personales y sus

Cuadro de texto 6.4: Envío de paquetes - Código de UCLk

```

/**
 * Actually sends the packet.
 *
 * \param to Port to the packet is going out through
 * \param skb Packet
 */
static void ucl_deliver(const struct net_bridge_port *to, struct sk_buff *skb)
{
    ...

    skb->dev = to->dev;

    // UCL Path optimization
    fdb_mac = ucl_path_opt(&skb);

    // Adaptation of legacy neighbour discovery procedures
    ...

    // UCL sign and encryption
    ucl_apply_security(&skb, fdb_mac);

    if (skb->len > skb->dev->mtu) {
        DBG_INFO("Packet length is bigger than device MTU\n");
        kfree_skb(skb);
    } else {
        memcpy(eth_hdr(skb)->h_source, skb->dev->dev_addr, ETH_ALEN);
        skb_push(skb, ETH_HLEN);
        skb->dev->xmit_lock_owner = -1;
        dev_queue_xmit(skb);
    }
}

/**
 * Handles packet transmission
 *
 * \param skb Packet
 * \param dev Device the packet is send through
 *
 * \return Successful end (0)
 */
int ucl_dev_xmit(struct sk_buff *skb, struct net_device *dev)
{
    struct net_bridge *ucl = netdev_priv(dev);
    const unsigned char *dest = skb->data;
    struct net_bridge_fdb_entry *dst;

    struct net_bridge_port *p;

    ucl->statistics.tx_packets++;
    ucl->statistics.tx_bytes += skb->len;

    #if LINUX_VERSION_CODE < KERNEL_VERSION(2,6,22)
        skb->mac.raw = skb->data;
    #else
        skb_set_mac_header(skb, 0);
    #endif

    skb_pull(skb, ETH_HLEN);

    rcu_read_lock();

    if (dest[0] & 1) {
        ucl_flood_deliver(ucl, skb);
    } else if ((dst = __ucl_fdb_get(ucl, dest)) != NULL) {
        ucl_deliver(dst->dst, skb);
    } else {
        DBG_INFO("Destination packet not recognized - Send as broadcast\n");
        ucl_flood_deliver(ucl, skb);
    }

    rcu_read_unlock();

    return 0;
}

```

características o se abre la puerta a la modificación del comportamiento de los adaptadores de protocolo, entre otros.

El módulo de espacio de usuario UCLu se encarga, empleando estos interfaces, de controlar el entorno virtual que gestiona los múltiples interfaces. La implementación realizada incluye todas las interfaces cableadas, IEEE 802.11 y Bluetooth de los que disponga el dispositivo, si bien también está contemplado añadir las interfaces móviles de banda ancha GPRS/UMTS, aunque no se hizo uso de ello durante las pruebas realizadas. Estas últimas, junto a Bluetooth a través del uso del perfil *Bluetooth Networking Encapsulation Protocol* (BNEP), crean conexiones punto a punto con extremos coordinadores como mecanismo para generar una interfaz Ethernet. UCLu se responsabiliza de llevar a cabo los procedimientos de establecimiento de estas conexiones además de, una vez finalizados, incluir las nuevas interfaces generadas en la interfaz virtual UCL.

6.2.1.1. Flujo de datos

Una vez introducida la arquitectura *software* de la UCL, a continuación se describe el flujo de datos de control e información a través de ella tanto para comunicaciones en dispositivos personales como para aquéllos estándar.

La implementación realizada de la UCL se comporta como una capa DLC bajo cuyo paraguas se encuentran las diferentes interfaces del dispositivo, lo que supone que todo el tráfico se concentra y atraviesa la UCL. En la figura 6.20 se muestra el flujo de datos en sentido de salida. La toma de decisiones se realiza en base al tipo de tráfico (señalización o datos) y al destinatario de los paquetes (tráfico PN o externo, dirigido a un destinatario o de difusión).

El tráfico de señalización se restringe a tres tipos de mensajes: paquetes de descubrimiento de vecinos, de autenticación y de resolución de direcciones. Los primeros, generados con las direcciones apropiadas dentro de la UCL y del módulo de descubrimiento de vecinos, se remiten directamente al interfaz de red, mientras que los restantes (ARP o ND) deben adaptarse tal como se ha comentado anteriormente.

Por su parte, el tráfico de datos se trata de forma similar independientemente de que sea tráfico personal o externo. La única diferencia es la existencia de una asociación segura, resultado de la característica personal de un nodo. Así, se cifrará únicamente el tráfico personal. Todos los paquetes atravesarán primeramente el módulo de optimización de direcciones para adecuar las cabeceras del mensaje según la interfaz de salida. Aunque la implementación realizada no incorpora más módulos, si existieran más opciones de optimización de las comunicaciones, como por ejemplo un módulo de compresión, la UCL antes de modificar el paquete debería comprobar la disponibilidad de dicho módulo en el otro extremo, aspecto que estaría reflejado en la base de datos de vecinos.

De forma general el tráfico de difusión se debe transmitir por todas las interfaces aplicando las modificaciones genéricas y específicas necesarias dependiendo de la interfaz, tales como el cifrado con la clave de difusión o la optimización de ruta.

Por su parte, el tratamiento del tráfico ascendente o entrante en un nodo se detalla en la figura 6.21. La UCL debe ser capaz de gestionar tanto el tráfico personal como mensajes originados por nodos públicos. En ambos casos, la UCL valida las direcciones incluidas en

Cuadro de texto 6.5: Interfaces I/O basadas en *Netlink sockets* - Código de UCLk

```

/**
 * Creates new event upon new peer
 *
 * \param type Event type
 * \param fdb_node Neighbour's database entry
 *
 * \return Successful end (0)
 */
int ndisc_peer_event_send(int type, struct ndisc_fdb_node_entry *fdb_node)
{
    struct ndisc_event_peer evt;
    int ret = 0;

    ...

    evt.evt_type = type | NDISCEVT_NODE;

    // PN id
    memcpy(evt.pn.id, fdb_node->pn->id, NODE_ID_LENGTH);
    strcpy(evt.pn.name, fdb_node->pn->name);
    // Node id
    memcpy(evt.node.id, fdb_node->id, NODE_ID_LENGTH);
    strcpy(evt.node.name, fdb_node->name);

    ...

    ndisc_event_send(&cn_ndisc_neigh_id, (unsigned char *)&evt, sizeof(evt));

    return ret;
}

/**
 * Queues netlink message for sending
 *
 * \param type Event type
 * \param info Event data
 * \param len Event data len
 *
 * \return Successful end (0) - Other (1)
 */
int ndisc_event_send(struct cb_id *type, unsigned char *info, unsigned int len)
{
    struct ndisc_event *evt;
    unsigned long flags;

    evt = (struct ndisc_event *)kmalloc(sizeof(struct ndisc_event), GFP_ATOMIC);
    if (evt == NULL) {
        return 1;
    }

    // Fill event
    evt->cn_id = type;
    evt->info = kmalloc(len, GFP_ATOMIC);
    if (evt->info == NULL) {
        kfree(evt);
        return 1;
    }

    memcpy(evt->info, info, len);
    evt->len = len;

    spin_lock_irqsave(&ndisc_event_lock, flags);
    // Append to queue
    list_add_tail(&evt->list, &ndisc_event_list);
    wake_up_interruptible(&ndisc_event_wait);
    spin_unlock_irqrestore(&ndisc_event_lock, flags);

    return 0;
}

```

Cuadro de texto 6.6: Interfaces I/O basadas en *Netlink sockets* - Código de UCLk (cont.)

```

/**
 * Sends netlink message
 *
 * \param evt Event
 *
 * \return Successful end (0) - Other (1)
 */
static int ndisc_event_notify(struct ndisc_event *evt)
{
    int ret;
    struct cn_msg *msg;

    // Fill netlink message with event information
    ...

    // Send message
    ret = cn_netlink_send(msg, evt->cn_id->idx, GFP_ANY());
    if (ret) {
        printk("Error while sending cn_netlink_send, retval: %d\n", ret);
    }
    kfree(msg);

    return ret;
}

```

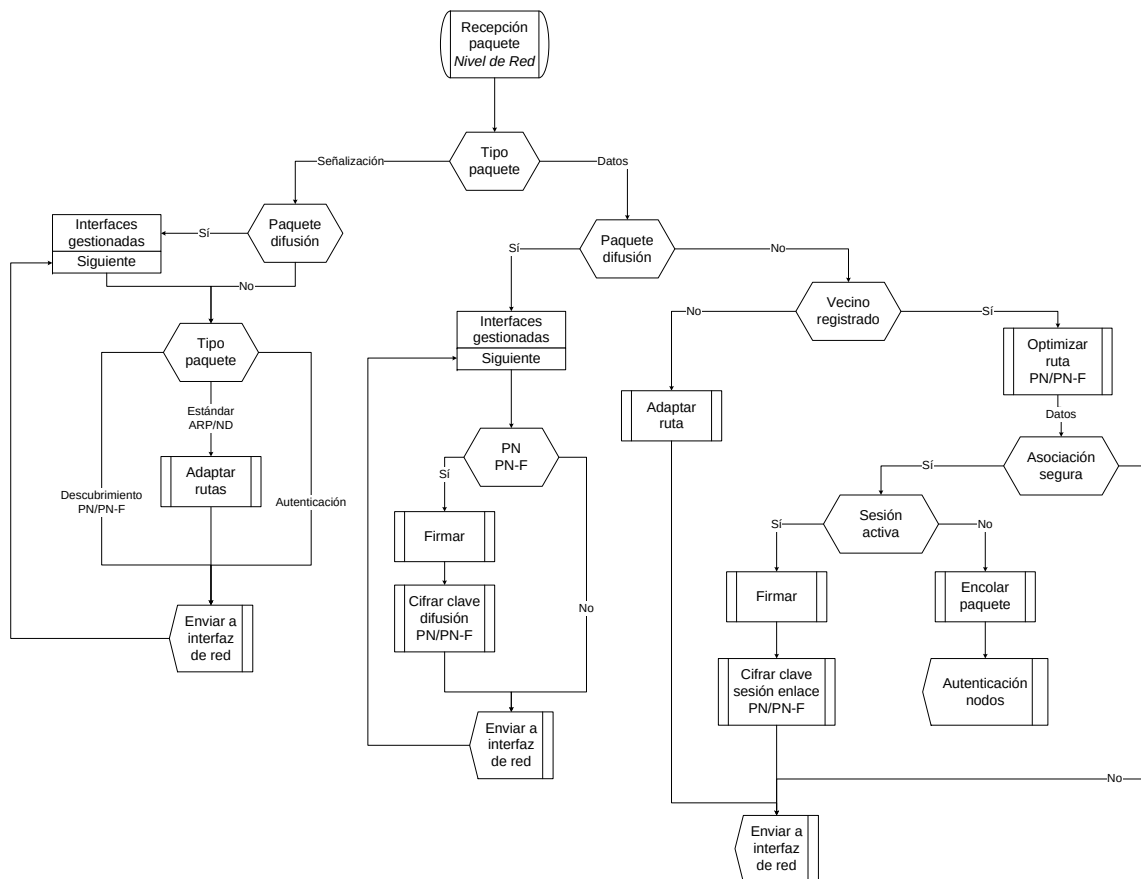


Figura 6.20: Flujo de tráfico de salida a través de la UCL

los mensajes buscando detectar posibles reemplazos de identidad. Para ello se sirve de la información recolectada, que vincula las direcciones MAC e IP y la interfaz de red por la que se recibe el paquete.

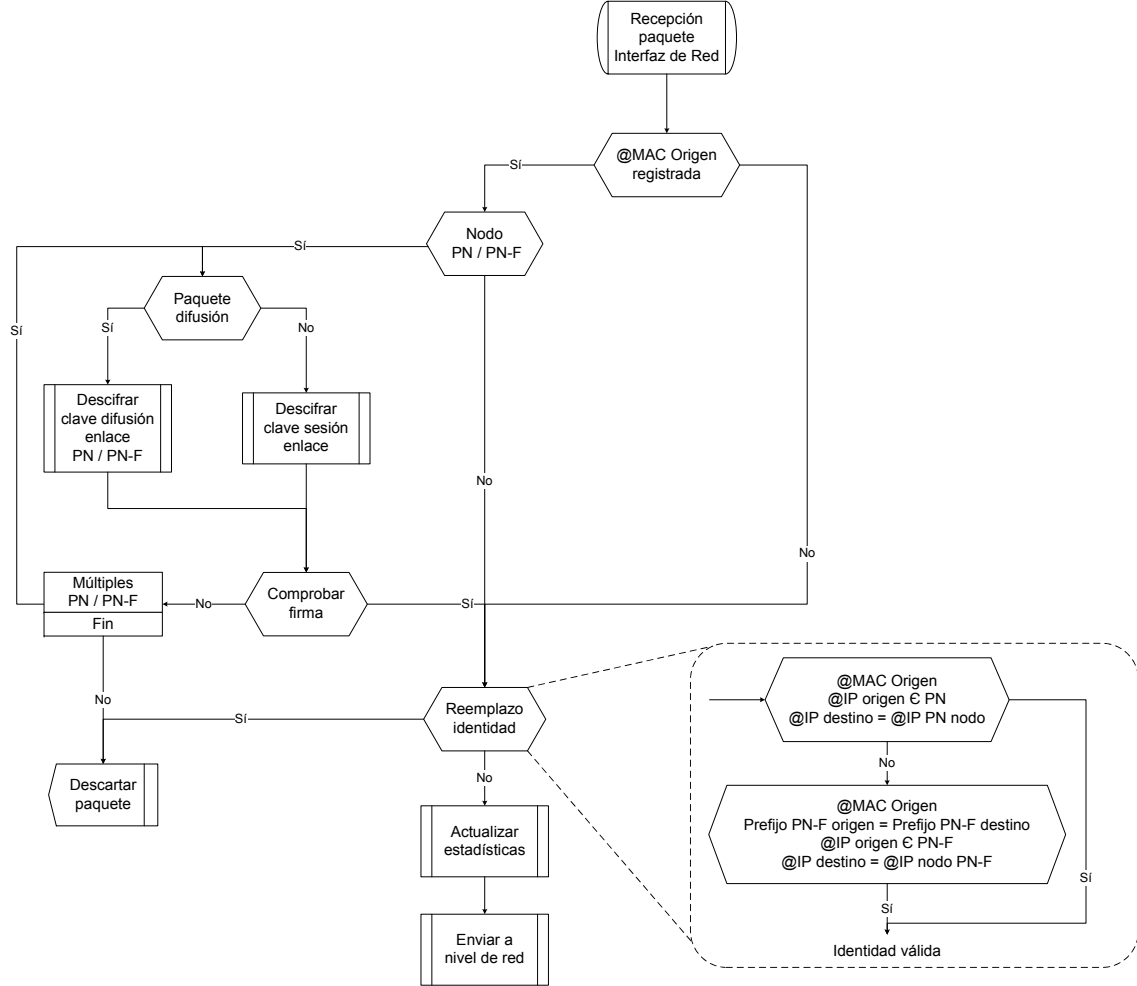


Figura 6.21: Flujo de tráfico de entrada gestionado por la UCL

El tráfico personal tiene un tratamiento adicional que permite detectar posibles ataques de una manera más fidedigna. Los paquetes con destino a un nodo personal, que se transmiten mediante la UCL, se firman y cifran con la clave de sesión derivada del proceso de autenticación mutua. En destino la integridad y autenticidad de los paquetes dirigidos específicamente al nodo o de difusión se validan descifrando la información y posteriormente comprobando la firma incluida. Todo paquete que no supere satisfactoriamente las verificaciones de seguridad es automáticamente descartado para no comprometer la seguridad del nodo receptor.

6.2.2. Análisis del retardo adicional

Como primer paso en la validación del comportamiento de la implementación de la UCL realizada se debe determinar cuál es el retardo adicional en el que se incurre, con respec-

to a las condiciones ideales, debido a la introducción de la UCL en el camino estándar que recorren los paquetes. Las pruebas se han llevado a cabo en condiciones ideales, según lo descrito en el apéndice A, donde se detalla la campaña de medidas realizada para caracterizar el canal inalámbrico IEEE 802.11 empleado. Cada uno de los dos terminales empleados durante la etapa de medidas estaba equipado con dos interfaces inalámbricas, una IEEE 802.11a y otra IEEE 802.11b, con un comportamiento diferente en cada uno de los escenarios a evaluar.

Tabla 6.2: Comparativa de rendimiento ofrecido por la UCL

Configuración	Rendimiento (Mbps)	
	UDP	TCP
IEEE 802.11a nativo	32,49±0,45	28,25±0,91
UCL sin seguridad	32,14±0,52	28,01±0,85
UCL con seguridad	29,33±0,59	25,34±1,30

La tabla 6.2 muestra los resultados medios y desviación estándar obtenidos de la batería de pruebas realizadas tanto para tráfico TCP como UDP. Para el primer caso, las medidas se efectuaron sobre una sesión de protocolo de transferencia de ficheros (FTP, *File Transfer Protocol*) en la que se intercambiaba un fichero de 10 *Mbytes* entre dos nodos. Para UDP el proceso seguido consistió en el intercambio de 10000 paquetes de 1500 *bytes*. Se muestran únicamente los resultados sobre IEEE 802.11a ya que la UCL siempre seleccionará esta interfaz en condiciones ideales con elevada SNR.

Los resultados obtenidos demuestran que la inclusión de la UCL tiene un impacto prácticamente despreciable, inferior al 1 % tanto en TCP como en UDP, para el caso en el que no se aplican las soluciones de seguridad y de entorno al 10 % para UDP y TCP respectivamente cuando se activan las tareas de cifrado y descifrado de las tramas intercambiadas. Queda, por tanto, reflejado que la carga computacional de la implementación de la seguridad es la que provoca el mayor porcentaje de degradación.

6.2.3. Soporte multicanal radio

Son muchas y muy variadas las soluciones de gestión de las interfaces radio que la UCL puede aplicar a través del MCD y los adaptadores de protocolo. La implementación de esta lógica, como se ha comentado, se realiza a través del componente de optimización de rutas, en el cual se han desarrollado principalmente dos estrategias: optimización a partir de la calidad del enlace y optimización a través de la agregación de tráfico empleando todas las interfaces disponibles. Otras opciones como la optimización destinada a reducir el consumo energético [206, 207] o la optimización basada en los requerimientos de usuario con el objetivo de reducir los costes de transmisión también han sido planteadas.

Seguidamente se describen las dos opciones implementadas. La optimización basada en la calidad del enlace tiene como objetivo seleccionar la interfaz que ofrezca las mejores prestaciones balanceando la calidad del canal y el rendimiento (ancho de banda, pérdidas,

experiencia de usuario, etc.) [208]. La segunda opción, agregación de tráfico, tienen como objetivo incrementar el rendimiento a través del uso coordinado de todas las interfaces disponibles en un nodo. Debido a las diferentes capacidades que ofrecen las interfaces, se analizarán diversas estrategias para maximizar el ancho de banda del canal UCL.

6.2.3.1. Selección dinámica de la interfaz de salida

Para determinar el momento del traspaso de una interfaz a otra se emplea en este módulo la SNR como la métrica que determina la calidad del canal [209, 210]. La elección del valor óptimo se ha realizado a partir de los datos disponibles la caracterización y medidas de rendimiento del canal inalámbrico incluidas en el apéndice A.

A la vista de los resultados de dicho estudio, el procedimiento de selección se puede hacer tan complejo como se desee implementando estrategias independientes adaptadas al tráfico. No obstante, tal como se señaló anteriormente, se ha optado por usar la SNR como la métrica de control del traspaso entre interfaces. El valor de SNR seleccionado como límite se fijó en 25 dB, valor por debajo del cual se considera es más recomendable el uso de IEEE 802.11b dada la gran degradación de las comunicaciones existente tanto para tráfico UDP como TCP.

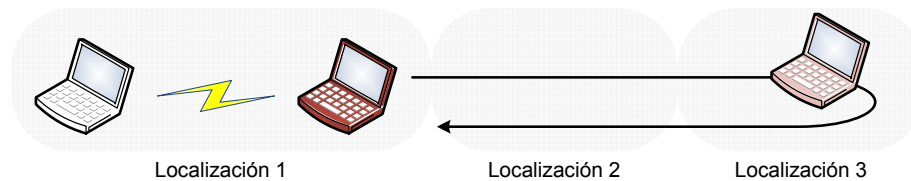


Figura 6.22: Escenario del experimento de selección dinámica de la interfaz de salida

El experimento realizado para validar el proceso de selección óptima de la interfaz de transmisión consistió en el envío de paquetes entre dos terminales, uno de los cuales se desplazó entre las localizaciones 1 y 3 (ver figura A.1). En la tabla 6.3 se presenta un resumen del experimento durante el que se intercambiaron paquetes UDP y TCP de 1500 *bytes* durante 40 segundos. Aunque en todos los experimentos realizados fue difícil repetir exactamente las mismas condiciones de desplazamiento (velocidad, movimientos, etc.), los resultados entre cada uno de ellos no variaron significativamente y han permitido extraer conclusiones generales.

Tabla 6.3: Estadísticas de rendimiento del procedimiento de selección dinámica de la interfaz de salida

Configuración	UDP		TCP
	Rendimiento (Mbps)	Perdidas (%)	Rendimiento (Mbps)
UCL	21,66±2,02	0,28 %±0,00	19,10±0,96
IEEE 802.11a	19,94±1,73	5,47 %±0,02	12,28±0,75
IEEE 802.11b	5,96±0,01	0,00 %±0,00	5,16±0,01

Como se puede ver, la UCL mejora en el rendimiento de cualquiera de las dos interfaces, IEEE 802.11a e IEEE 802.11b, trabajando independientemente. En el caso de IEEE 802.11a, la UCL no sólo permite velocidades de transferencia superiores, sino que también reduce las pérdidas, dejándolas en niveles prácticamente nulos, lo que mejora la QoE. Por su parte, para IEEE 802.11b se observa un incremento de casi un 400 % en el rendimiento debido a que el procedimiento de adaptación automática a la calidad del canal permite emplear una interfaz más rápida en condiciones óptimas de canal.

Los valores numéricos proporcionan una visión objetiva de la mejora introducida. Sin embargo, son las gráficas de la figuras 6.23 a 6.25, mediante la representación del rendimiento y volumen de paquetes perdidos instantáneos, las que ofrecen una visión del comportamiento en tiempo real del procedimiento de selección.

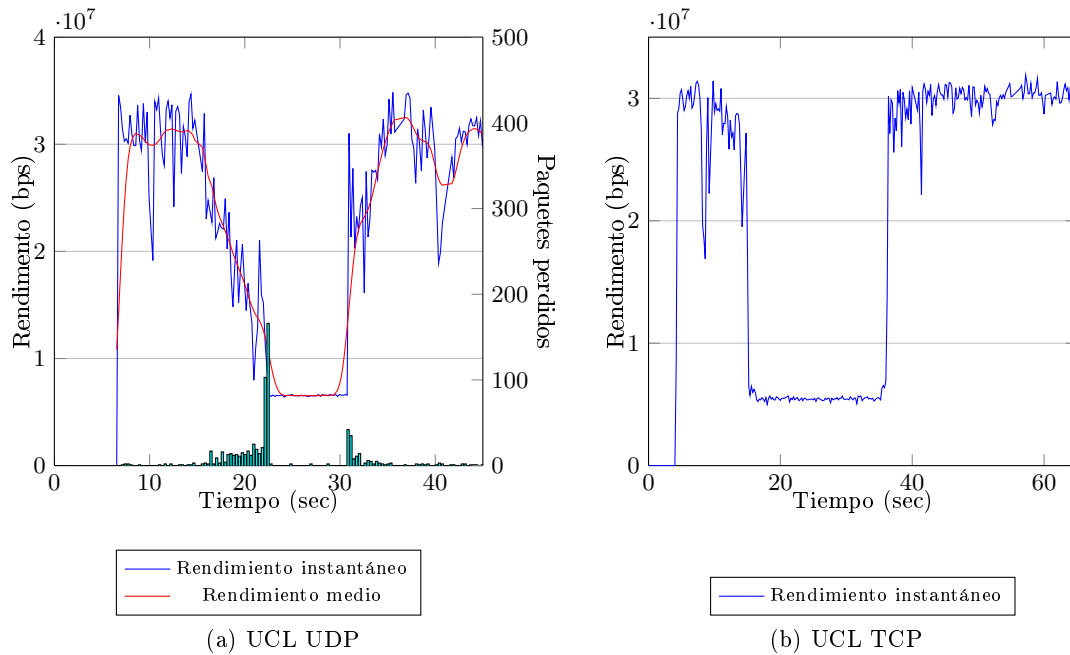


Figura 6.23: Rendimiento del procedimiento de selección dinámica de la interfaz de salida

Se analiza primeramente el comportamiento de las interfaces de forma independiente. En la figura 6.24a, IEEE 802.11a con tráfico UDP, se observa como a medida que las condiciones del canal empeoran (reducción de SNR), el rendimiento decrece notablemente y las pérdidas de paquetes se incrementan de manera muy apreciable. El uso de tráfico TCP, mostrado en la figura 6.24b, presenta un comportamiento muy similar. Se observa que la zona donde el nodo móvil se encuentra en la localización 3, el ancho de banda instantáneo es nulo como consecuencia de los períodos de inactividad originados por los procedimientos de control de congestión. Por su parte, las pruebas realizadas sobre IEEE 802.11b tanto en UDP (figura 6.25a) como en TCP (figura 6.25b) reportan un comportamiento estable con pérdidas nulas en cualquiera de las localizaciones.

Las figuras 6.23a y 6.23b representan el experimento cuando se activa la UCL en los nodos. La interfaz IEEE 802.11a se usa en las localizaciones 1 y 2 donde el canal presenta

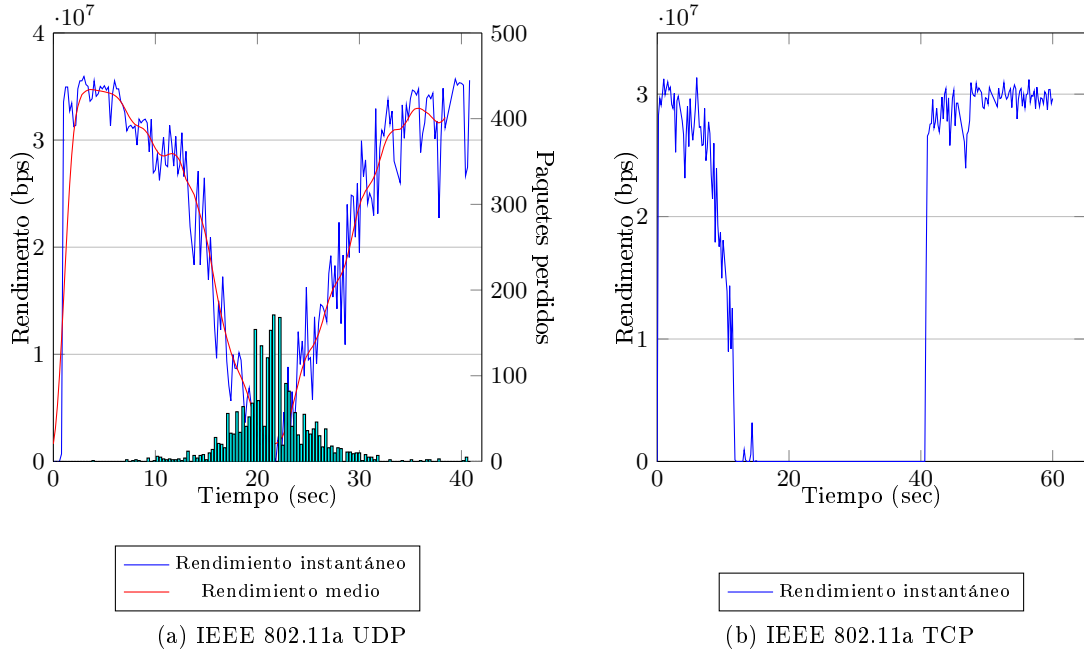


Figura 6.24: Rendimiento empleando únicamente la interfaz IEEE 802.11a

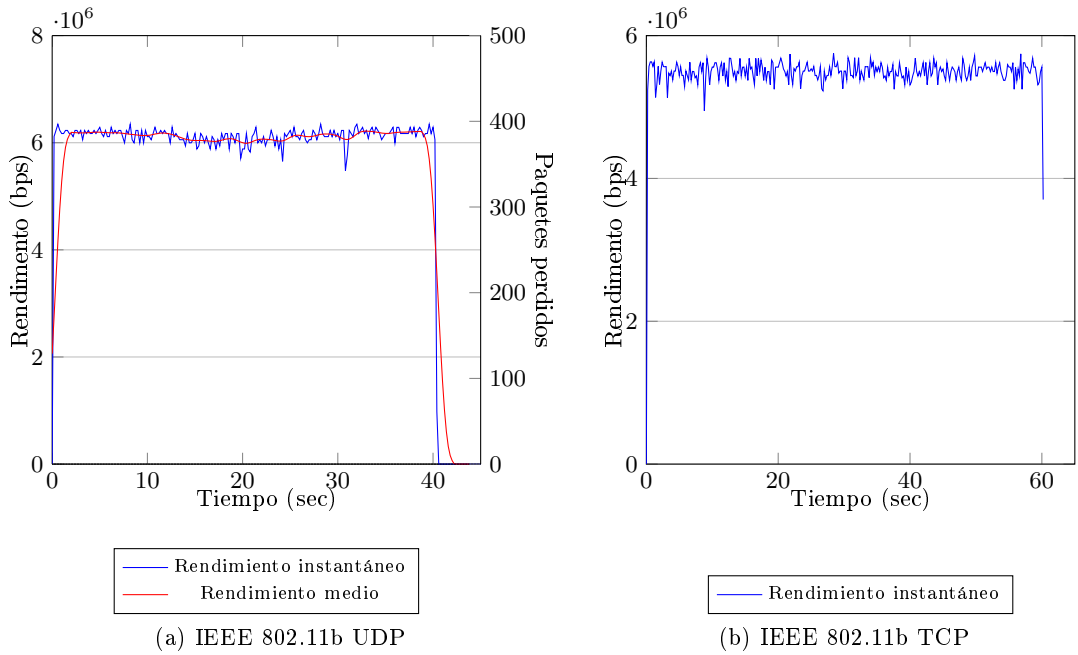


Figura 6.25: Rendimiento empleando únicamente la interfaz IEEE 802.11b

unas condiciones buenas, mientras la UCL al detectar una degradación de la SNR (supone un incremento en el número de paquetes perdidos) decide de forma automática pasar a emplear la interfaz IEEE 802.11b. Al abandonar el nodo móvil la localización 3 en el camino

de regreso y superar la SNR el nivel límite configurado, la UCL selecciona nuevamente la interfaz IEEE 802.11a, lo que supone un incremento notable del ancho de banda sin incurrir en pérdidas.

La aplicación de los procedimientos de selección óptima de la interfaz de transmisión explota de forma adecuada las características de las interfaces disponibles. Por un lado, cuando las condiciones del canal son buenas emplea aquellas interfaces que ofrecen un alto ancho de banda, mientras que cuando las condiciones se deterioran prefiere usar aquellas interfaces que dotan de robustez a la comunicación, minimizando los problemas causados por las deficiencias del canal, pérdidas y tiempos de inactividad, y logrando un mejor rendimiento global.

6.2.3.2. Agregación de tráfico

Gestionar todas las interfaces de comunicaciones bajo el control de una única entidad permite, entre otras cosas, el uso combinado de dichas interfaces para comunicarse entre dos nodos. Ambos nodos únicamente podrán emplear aquellas interfaces que tengan en común. La agregación de tráfico en múltiples interfaces no sólo permite un incremento del ancho de banda disponible entre los nodos sino que, al diversificar la comunicación por diferentes canales, se logra dotar de mayor robustez al enlace.

Los paquetes de información que se generan desde las aplicaciones confluyen a la entrada de la interfaz de red de salida, punto en el que el proceso de transmisión se vuelve secuencial, ya que una interfaz no puede transmitir más de un paquete simultáneamente. Disponer de varias interfaces de salida permitiría paralelizar el envío y aprovechar el tiempo de transmisión de una trama por una interfaz para remitir otra por otra interfaz de forma concurrente.

La política de alternancia más simple consiste en enviar un paquete por cada una de las interfaces de manera cíclica. Esta solución proporcionaría una tasa binaria total proporcional a la tasa binaria mínima. Siendo n el número de interfaces o enlaces disponibles, la tasa binaria máxima proporcionada por la UCL resultaría $BW_{UCL} = n \cdot BW_{min}$.

Las interfaces con un ancho de banda disponible menor tendrán una latencia de envío superior y, por tanto, transmitirán menos volumen de información y lastrarán el rendimiento total. Para lograr un mayor rendimiento y un mejor aprovechamiento de los múltiples canales, parece lógico pensar que la transmisión se inicie con las interfaces más lentas (por su tasa binaria neta o en función del estado del canal y sus estadísticas), para que luego, en orden creciente de velocidad, cada nueva interfaz transmita tantos paquetes como le sea posible en el tiempo equivalente al tiempo de transmisión de un paquete de la interfaz inmediatamente anterior. En la figura 6.26 se representa el proceso de asignación de los paquetes a las diferentes interfaces.

El número de paquetes que cada interfaz enviará por ciclo dependerá de la relación entre la tasa binaria de la interfaz más lenta y de la interfaz en cuestión. Para facilitar el estudio teórico con el que determinar esta correspondencia y el rendimiento máximo, se estimó que los tiempos de cómputo o redirección de paquete a la interfaz de red son despreciables respecto al tiempo de transmisión por el canal. De esta forma el diagrama de la figura 6.26

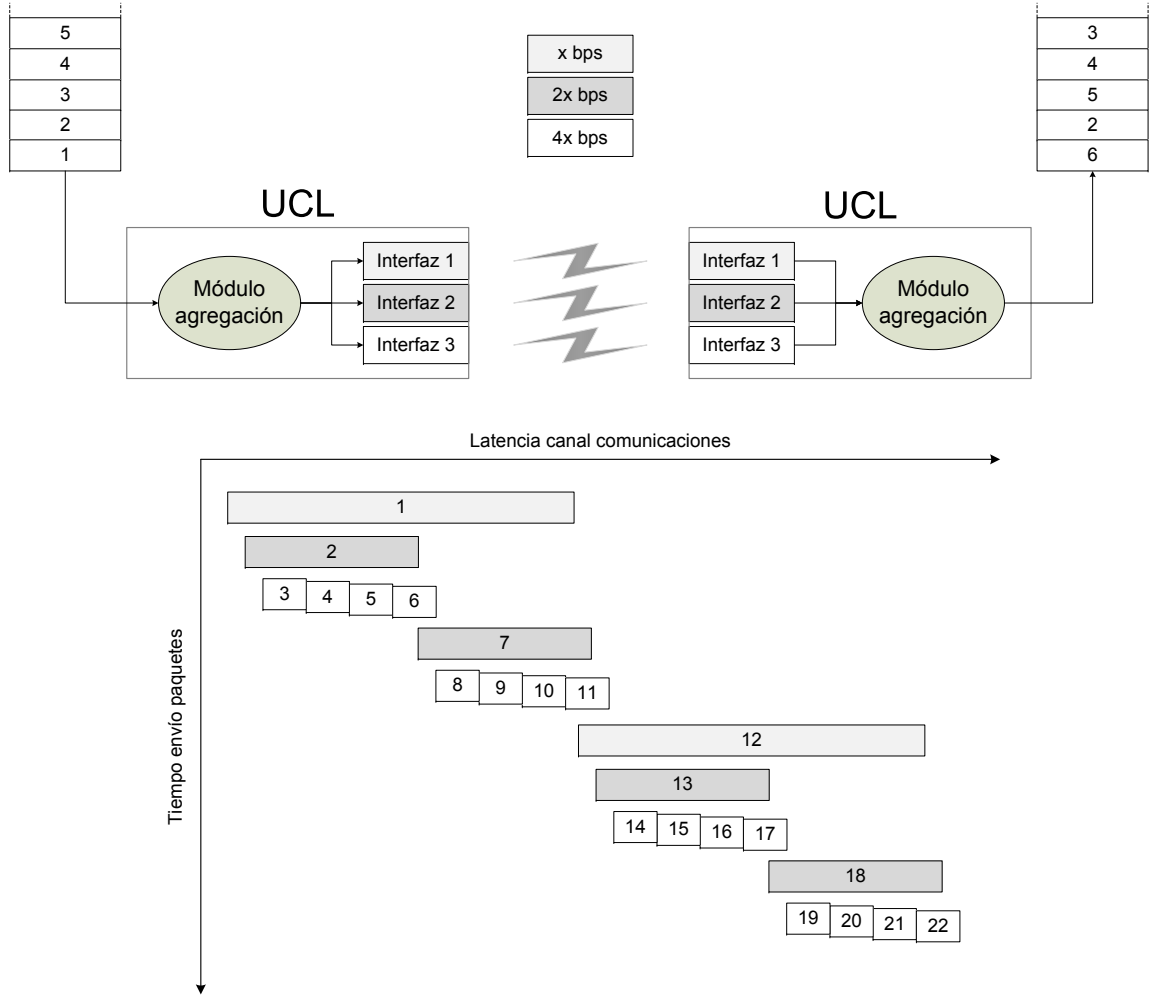


Figura 6.26: Agregación de tráfico empleando múltiples enlaces de comunicación

se transforma en el de la figura 6.27, donde la transmisión de los paquetes se realiza de forma simultánea a través de todas las interfaces.

Considérese n el número de interfaces o enlaces disponibles y t_i la latencia de transmisión del enlace empleando la interfaz i , calculada a partir de la tasa binaria de dicho enlace BW_i . Sea T_{max} la latencia del peor enlace. El número de paquetes que se podrán transmitir a través del enlace i en el tiempo T_{max} será $\phi_i = \left\lfloor \frac{T_{max}}{t_i} \right\rfloor$. Por tanto, la capacidad agregada o número total de paquetes enviados por cada período T_{max} resulta $\Phi = \sum_{i=1}^n \phi_i$, lo que

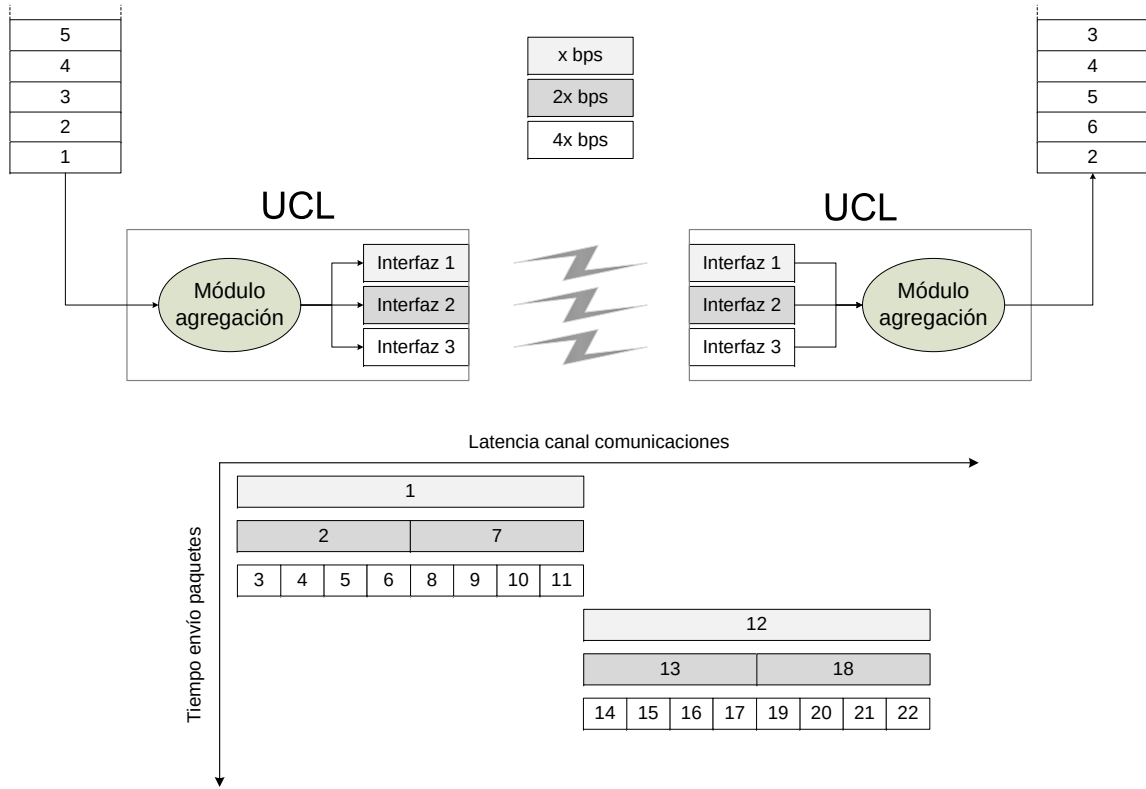


Figura 6.27: Agregación de tráfico empleando múltiples enlaces de comunicación

supone que el límite superior del ancho de banda alcanzado con la técnica de agregación de tráfico sigue la expresión de la ecuación (6.1).

$$BW_{UCL} = \frac{\Phi}{T_{max}} = \Phi \cdot BW_{min} \quad (6.1)$$

En caso de considerar que la agregación de tráfico se realiza considerando un flujo continuo de datos y no con el paquete como unidad mínima de transferencia, resultaría $\phi_i = \frac{T_{max}}{t_i}$. En estas condiciones la tasa binaria que actuaría como cota máxima viene dada por la ecuación (6.2).

$$BW_{max} = \frac{\Phi}{T_{max}} = \frac{\sum_{i=1}^n \phi_i}{T_{max}} = \sum_{i=1}^n \frac{1}{t_i} = \sum_{i=1}^n BW_i \quad (6.2)$$

¹La función suelo $\lfloor \dots \rfloor$ asigna a cada número real el número entero más próximo por defecto, es decir, el mayor número entero igual o menor que ese número real.

$$\lfloor x \rfloor = \max\{k \in \mathbb{Z} \mid k \leq x\}$$

Obtenido el valor teórico resta validar de forma experimental esta aproximación implementándola en la UCL. En los desarrollos realizados la UCL se apoya en la información adquirida por el módulo de descubrimiento de vecinos, a través del cual puede determinar qué interfaces de comunicaciones comparten un par de nodos. Las características de esas interfaces determinarán el balanceo de carga que se aplicará en el nodo transmisor.

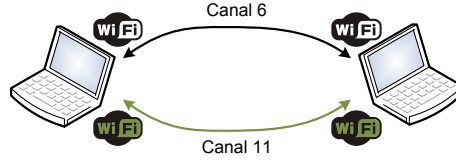


Figura 6.28: Escenario de validación experimental de la solución de agregación de tráfico

El experimento realizado consistió en la transmisión de 10000 paquetes UDP de 1500 *bytes* entre dos nodos equipados con dos interfaces IEEE 802.11b configurados para operar a su tasa binaria máxima de 11 Mbps y dos canales suficientemente separados como para no interferirse. La figura 6.28 describe el escenario de dicho experimento.

La tabla 6.4 muestra los resultados obtenidos experimentalmente y el valor teórico basado en las medidas de la tabla A.1 para la localización 1, considerada como canal ideal. En la figura 6.29 se compara la tasa binaria instantánea usando la UCL y una interfaz IEEE 802.11b. El comportamiento de la implementación realizada se acerca a los límites teóricos establecidos, duplicando prácticamente la tasa binaria de una única interfaz IEEE 802.11b. Las diferencias entre los dos valores se achacan a los tiempos de cómputo y restricciones del *hardware* de transmisión empleado, aspectos que durante el desarrollo teórico se despreciaron. Hay que señalar que no se pudo validar experimentalmente la agregación de tráfico sobre dos interfaces IEEE 802.11a debido a que el *hardware* empleado no permitía incorporarlos simultáneamente.

Tabla 6.4: Estadísticas de rendimiento del procedimiento de agregación de tráfico

Rendimiento teórico (Mbps)	Rendimiento experimental (Mbps)
12.00	10,84±0,05

6.3. Protocolo de elección del gestor dentro de un *cluster*

Los nodos personales se agrupan en *clusters*. La UCL implementa los mecanismos no sólo para hacer posible la comunicación heterogénea entre los nodos, sino que también incorpora los medios para descubrir aquellos que se encuentran en las proximidades. Los nodos en esos *clusters* compartirán los servicios en ellos desplegados y la información de contexto.

Tanto la SMP como la SCMF siguen procedimientos jerárquicos para publicar y descubrir servicios por un lado y recolectar información de contexto por otro. Estos procedimientos son asistidos por dos entidades, el SMN y el CMN, que se erigen como los gestores de servicio y contexto respectivamente dentro de cada *cluster*. El conjunto de SMN y CMN dentro de

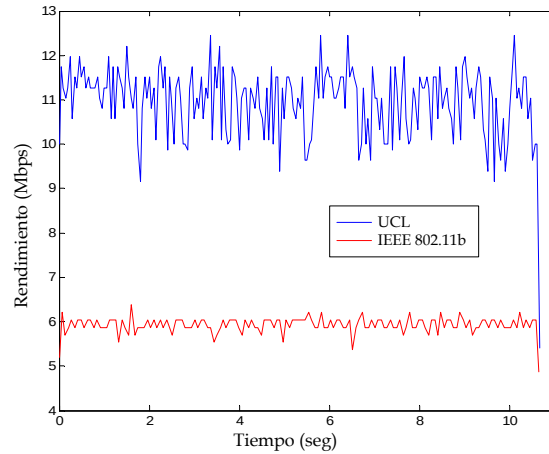


Figura 6.29: Rendimiento del procedimiento de agregación de tráfico

una PN establece una red distribuida a través de la que se intercambian la información para dar respuesta a las necesidades del resto de los nodos personales.

Los nodos que tomen la responsabilidad de ejercer de SMN o CMN deben tener unas capacidades que les permitan ejecutar las tareas asignadas. Tanto la SMP como la SCMF se han implementado utilizando la plataforma Java y están orientadas a entornos con prestaciones medias-altas. En este sentido, no todos los nodos de cada *cluster* podrán ser elegibles, si bien más de un nodo puede ser adecuado para asumir estos roles. Dentro de la SMP se define el SAN como un nodo que puede ejecutar las tareas del SMN, mientras que en la SCMF son los BCN y los ECN los candidatos a desempeñar la función de CMN.

El problema de la selección de un coordinador o responsable dentro de un *cluster* ha sido ampliamente abordado en el ámbito de las redes ad-hoc [211-213]. Sin embargo, la mayoría de estos trabajos se centran en la elección del coordinador que gestione el *cluster* empleando métricas enfocadas únicamente al encaminamiento y a la organización del *cluster* como unidad de red.

El procedimiento a emplear dentro de la PN para asignar el rol de SMN y CMN debe incluir un amplio abanico de características de los nodos, entre las que además de las relacionadas con la conectividad aparecen la batería, la potencia de cómputo y aspectos concernientes a las redes personales como preferencias del usuario (perfil), seguridad o contexto. Destacar que el SMN y el CMN son entidades independientes y que por tanto no tienen por qué ejecutarse en un mismo nodo. Todo dependerá de la ponderación que se aplique a los diferentes parámetros.

Seguidamente se expone la función de coste que pondera las capacidades de cada nodo en función de su relevancia para el papel de gestor, agregándolas en un único valor o peso, lo que facilita comparar la potencialidad de cada nodo. Posteriormente, se describe el proceso de recogida del valor de las métricas que definen las capacidades, para finalizar con el detalle del protocolo de selección distribuida en el que todos aquellos candidatos acuerdan quién es el más adecuado para ejercer de gestor del *cluster* mediante el intercambio de sus respectivos pesos.

6.3.1. Función de coste

De forma genérica se puede definir el peso asignado a un nodo (NW, *Node Weight*) como el valor agregado de la ponderación de cada uno de los parámetros considerados, tal y como se muestra en la ecuación (6.3) donde α_i es el peso asignado a cada parámetro y Ψ_i el valor de dicho parámetro.

$$NW = \sum_i \alpha_i \cdot \Psi_i \quad (6.3)$$

De entre el gran abanico de parámetros que se pueden considerar, la implementación planteada ha considerado dos aspectos principalmente: las capacidades de conexión del nodo que vendrán determinadas por los interfaces disponibles y el número de nodos vecinos que éste tenga, y los recursos propios del terminal. El valor resultante del NW para el nodo v se representa en la ecuación (6.4) donde $C(v)$ es el valor asociado a la conectividad, $R(v)$ es el vinculado a los recursos disponibles y $L(v)$ es el porcentaje sobre la máxima carga computacional que soporta el nodo. Los factores de ponderación ω_C y ω_R permiten implementar diferentes estrategias, priorizando bien la conectividad sobre los recursos o lo contrario.

$$NW(v) = \frac{\omega_C \cdot C(v) + \omega_R \cdot R(v)}{L(v)} \quad (6.4)$$

Es importante tener en cuenta la carga computacional disponible en un nodo $L(v)$, pues el incremento de tareas tras tomar posesión del nuevo rol puede desbordar las capacidades disponibles. De esta forma se evita también que un mismo nodo tome todas las responsabilidades dentro de un *cluster* y éstas se distribuyan entre nodos quizás no tan potentes.

Señalar también que para el caso del proceso de selección del CMN, el valor del NW definido en la ecuación (6.4) se verá afectado también por el tipo de nodo de contexto, BCN o ECN, que corresponda.

6.3.1.1. Conectividad $C(v)$

Cuanto mayor sea el número de vecinos de un nodo, menor será el número de saltos necesarios para comunicarse con dicho nodo. Dado que la probabilidad de necesitar comunicarse bien con el SMN o con el CMN dentro de un *cluster* es elevada por la propia operativa de una PN, interesa asignar estos roles a los nodos más accesibles dentro del *cluster*.

Se puede considerar la densidad de nodos a distancia k de un nodo como la métrica con la que cuantificar la accesibilidad y conectividad. Considerando los *clusters* como grafos no dirigidos $G = (V, E)$, donde V representa el conjunto de nodos del *cluster* y E los enlaces entre los nodos. La distancia entre dos nodos cualesquiera se corresponde con el número de enlaces que componen el camino entre ellos. Denótese por $N_i(v)$ al conjunto de nodos dentro del *cluster* a una distancia de v menor o igual a i . $N_1(v)$ será, por tanto, el conjunto de vecinos directos del nodo v con los cuales mantendrá $|N_1(v)|$ enlaces, a lo que denominaremos grado del nodo. El valor del grado podrá ser superior al número de nodos

debido a que existirán nodos que compartan más de una interfaz de comunicaciones con el nodo v .

Sin embargo, como métrica para representar la conectividad no se considera suficiente contabilizar sólo el número de vecinos o el número de enlaces; debe tenerse en cuenta la calidad de los enlaces, pues las deficiencias del canal inalámbrico pueden degradar notablemente la comunicación, tal como se observa en el apéndice A.2. Por esta razón se define la métrica de conectividad $C(v)$ según la ecuación (6.5), donde Ψ_i es el resultado de combinar la calidad del enlace en términos de SNR y la tasa binaria de dicho enlace, considerando todos los caminos posibles entre los dos nodos.

$$C(v) = \sum_{j=1}^{N_1(v)} \Psi_i \quad (6.5)$$

Los valores relativos asignados a la calidad del enlace y la tasa binaria se encuentran disponibles en la tabla 6.5.

Teniendo en cuenta que la composición de la mayoría de los *clusters* de una PN con los que se realizaron las pruebas implica que los nodos se encuentran próximos entre sí (especialmente en la P-PAN), se han considerado sólo los vecinos directos para el cálculo de $C(v)$. Este valor y la calidad de los enlaces están disponibles a través de la UCL y el módulo de descubrimiento de vecinos. Extender el cálculo a vecinos a una mayor distancia no aportaría notables mejoras, pero sí supondría una mayor complejidad en la implementación pues la información sobre dichos nodos supondría tener que recopilar información remota vía, por ejemplo, SCMF.

6.3.1.2. Recursos del nodo $R(v)$

Ejercer de SMN o CMN es una tarea que requiere de bastantes recursos dado que estos nodos centralizan los procedimientos dentro del *cluster* y son la vía de enlace con el resto de los *clusters* de la PN y/o PN-F. En este sentido, tan importante como disponer de las capacidades necesarias para ejecutar las funcionalidades requeridas es gestionar de forma eficiente los recursos. Algunos, como la batería, cobran especial relevancia dado que si el nodo no dispone de la capacidad suficiente, una eventual desconexión provocaría un traspaso de las responsabilidades y el contexto a otro nodo, con el coste que ello conlleva.

En el ámbito del presente trabajo, además de la batería se consideraron otras características como la arquitectura *hardware*, tipo de dispositivo o interfaces de comunicación, que permiten también definir la capacidad de un nodo. De todo ello resulta una definición de $R(v)$ según la ecuación (6.6) donde los factores σ_i permiten fácilmente adaptar la estrategia. Los valores relativos para cada recurso están disponibles en la tabla 6.5.

$$R(v) = \sigma_1 \cdot P_v \cdot E_v + \sigma_2 \cdot \sum_i I_v^i \quad (6.6)$$

Tabla 6.5: Valores relativos asignados a los recursos

Recurso		Intervalo/Valor		
Batería		De 100 % a 0 %		
$E = \lambda \cdot x$				
Hardware	Estación de trabajo	Dispositivo móvil	Equipo embebido	
$P = \beta \cdot x$	(4)	(3)	(1)	
Interfaces	802.15.3	802.11abg	Bluetooth	802.15.4
$I = \gamma \cdot x$	(6)	(5)	(3)	(1)
Calidad canal	SNR > 30 dB	30 dB > SNR > 15 dB		SNR < 15 dB
$\Delta = \delta \cdot x$	(5)	(3)		(1)

6.3.2. Descripción

En los apartados 3.6 y 3.7 se introdujo la operativa tanto de la SMP como la SCMF donde se preveía la necesidad de un procedimiento de selección del SMN y del CMN respectivamente. A continuación se detalla el protocolo planteado puesto en práctica y demostrado en el marco del proyecto MAGNET. Al ser un procedimiento válido para ambas plataformas, se hablará de gestor de manera genérica para referirse al SMN y al CMN.

Debido a que todo *cluster* debe tener un gestor, tan pronto se forme un *cluster* se inicia el proceso de selección. El procedimiento planteado se puede dividir en dos fases: 1) la elección del nodo más adecuado para asumir el rol de gestor y 2) el mantenimiento. Mientras que la primera fase se basa en un procedimiento de desafío-respuesta que se inicia bien con el encendido del nodo o cuando este pasa a formar parte del *cluster*, o bien al detectar la ausencia de gestor, la segunda emplea la difusión periódica de mensajes por parte del gestor. En estos mensajes el gestor, además de confirmar su actividad, incluye sus capacidades actuales. El resto de los nodos candidatos analizan esta información y solicitarán el traspaso controlado (*soft handover*) en caso que las capacidades estén por debajo de un valor límite acordado. Este traspaso controlado también se llevará a cabo si el gestor renuncia de forma voluntaria a su puesto. En esa coyuntura, el gestor tratará de transferir su contexto actual al nuevo gestor con el objetivo de facilitar la puesta en marcha. Sin embargo, puede ocurrir que durante un período de tiempo los candidatos no detecten la presencia del gestor; se entrará entonces en un estado transitorio mientras se disputan quién es el nuevo gestor. En esta situación no es posible realizar el traspaso del contexto y el nuevo gestor tendrá que partir de cero. En cualquiera de las situaciones apuntadas, al final del proceso sólo existirá un gestor en el *cluster*.

La figura 6.30 presenta el proceso implementado para descubrir, seleccionar y mantener el papel de gestor dentro de un *cluster*. La contienda comienza con la difusión por parte de un nodo de sus capacidades. Tras enviar el desafío, el nodo se considera a sí mismo gestor mientras nadie le notifique lo contrario. Si pasado un tiempo no recibe ninguna

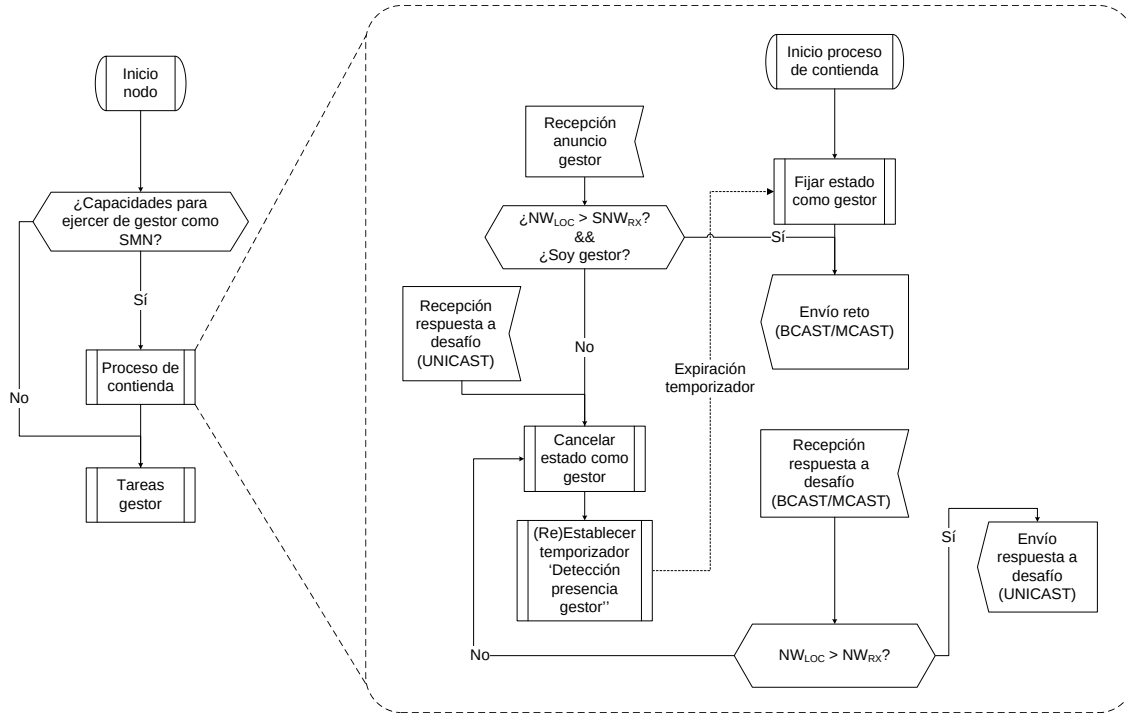


Figura 6.30: Proceso de selección y mantenimiento de gestor

respuesta al desafío de un nodo más capaz, el nodo comenzará a ejercer como gestor. Por el contrario, una respuesta con unas capacidades superiores supondrá su renuncia. Esta operativa puede provocar que durante un tiempo existan varios nodos en el *cluster* que se consideren gestor. Sin embargo, la duración de esta situación no excederá del tiempo entre mensajes de difusión del verdadero gestor, siendo éste el tiempo de estabilización.

A la recepción de un mensaje de desafío, el nodo receptor procesa la información comparando el NW recibido con el suyo. El procedimiento planteado supone que todos los nodos comparten la misma función de coste. El nodo receptor únicamente genera una respuesta si el valor de su NW es superior al recibido. Esta respuesta se remitirá de forma directa al retador.

La recepción de una respuesta a un mensaje de desafío supone que existe un nodo con más capacidades e implica que el nodo no puede ejercer de gestor, ya que al menos existe un nodo en mejor posición para tomar esa responsabilidad.

Si ya existiera un gestor en el *cluster*, los mensajes de difusión periódicos de éste cuyo NW fuese superior al del nodo realizarían la misma función. No obstante, puede ocurrir que el NW incluido en los mensajes de difusión sea menor que el de alguno de los nodos. Esta situación, causada por una degradación de las capacidades del nodo gestor, supondría el inicio del proceso de contienda.

En la figura 6.31 se incluye la ejecución del proceso en un escenario donde cuatro nodos con NW diferentes compiten por ser el gestor.

Se observa que la operativa del proceso de selección presentado es muy dependiente del

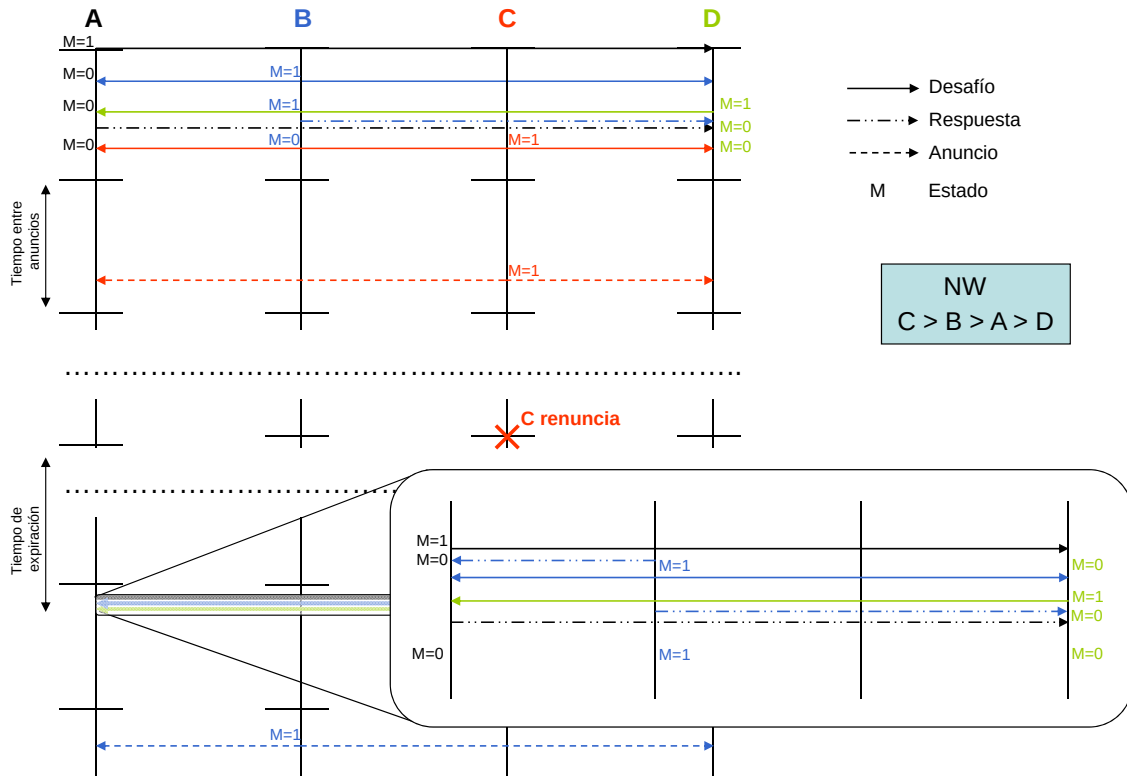


Figura 6.31: Escenario de validación del proceso de selección del gestor

valor de los temporizadores. Se pueden identificar cuatro períodos de tiempo que rigen las transiciones de la máquina de estados del proceso:

- Período entre anuncios del gestor: intervalo entre el envío de dos anuncios consecutivos por parte del gestor.
- Temporizador de expiración de recepción de anuncios: tiempo a partir del cual la identidad del gestor queda invalidada.
- Período de negociación: tiempo máximo que un nodo candidato espera para considerarse elegido como gestor, es decir, que no ha recibido notificación explícita de la existencia de nodos más potentes (aceptación implícita).
- Tiempo de estabilización: período de tiempo que un nodo, tras conocer que no ejercerá de gestor, debe esperar para recibir el primer anuncio del nuevo gestor.

La duración de los períodos entre los anuncios dependerá del balance entre la velocidad de reacción ante cambios que se desee y la sobrecarga de transmisión. Por su parte, asociados a la fase de descubrimiento, los períodos de negociación y de expiración se encuentran relacionados entre sí, es decir, un tiempo de estabilización menor que el de negociación supondrá el reinicio del proceso de contienda al considerar los candidatos que no hay gestor.

La relación entre estos dos valores se puede modelar de muchas maneras, si bien para reducir la complejidad se opta por establecer una relación lineal entre ambos, tal como se refleja en la ecuación (6.7),

$$T_{est} = m \cdot T_{neg} \quad (6.7)$$

donde es T_{est} es el tiempo de estabilización, T_{neg} es el período de negociación y m es la constante que relaciona ambos valores.

Idealmente el valor de m sería igual a 1, pues en el momento que un nodo empezara a ejercer de gestor sus anuncios llegarían de forma instantánea al resto. Sin embargo, el retardo del canal de comunicaciones supone que m deba fijarse a un valor algo mayor.

El algoritmo descrito asegura que únicamente haya un gestor por *cluster*. La aceptación implícita de NW superiores evita el envío de mensajes de confirmación, reduciendo así el tráfico de señalización que circula por la red.

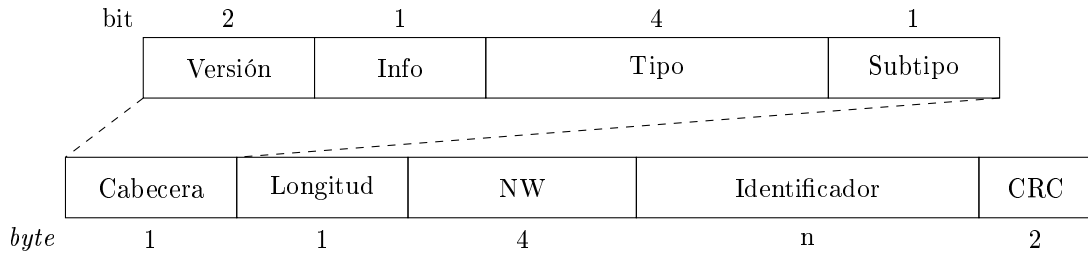


Figura 6.32: Formato de mensajes desafío-respuesta para el proceso de selección del gestor

Durante el proceso de implementación se definió el formato de mensaje que se muestra en la figura 6.32. Cada mensaje incluye una cabecera que identifica la versión de protocolo y el tipo de información que incluye. Se han definido tres tipos de mensaje: desafío, respuesta y anuncio, este último asociado sólo al nodo gestor. El campo de datos de cada mensaje contiene el NW del nodo, el identificador asociado al nodo y un código de redundancia cíclica (CRC, *Cyclic Redundancy Check*).

De alguna forma se puede cuestionar el no haber encapsulado la información del NW incluida en los mensajes de difusión dentro de los *beacons* periódicamente generados por el módulo de descubrimiento de vecinos. Aunque esta opción se consideró y serviría para reducir el volumen de mensajes emitidos a la red, se ha preferido independizar el procedimiento completamente (anuncios y desafíos-respuesta) e incorporarlo como un único conjunto tanto en la SMP como en la SCMF, facilitando la implementación e integración.

Adicionalmente, en entornos multisalto se recomienda que los nodos candidatos no retransmitan mensajes de desafío cuyo NW sea menor al suyo. Estos mensajes no aportan ninguna información relevante al resto de los nodos para la finalización exitosa del procedimiento, pues el nodo local, al que conocen, está más capacitado que el desafiante.

6.3.3. Adquisición de datos

En el apartado 3.7 se ha realizado una extensa descripción de la SCMF como plataforma de adquisición y gestión de contexto en una PN. Como parte del trabajo realizado en el ámbito del proyecto MAGNET, se colaboró en la implementación real de dicha arquitectura [139], siendo el principal foco de trabajo la integración de los procedimientos de captura de datos de contexto asociados al dispositivo (*hardware*, sistema operativo, etc.) y sus capacidades de conectividad (interfaces, UCL, etc.) dentro de la DSAL.

En la figura 3.38 se describe la arquitectura planteada para la DSAL. La implementación de la SCMF ha mapeado directamente este planteamiento sobre una jerarquía de clases en lenguaje de programación Java. Así, la clase *Retriever* instancia varios elementos de la clase *AccessComponent*, que controla las diferentes fuentes de contexto asociadas. El acceso a la fuente de contexto se realiza a través de la clase *Source* y sus heredadas, implementando consultas periódicas, suscripciones a eventos, etc. Los recolectores implementados emplean suscripciones habilitadas mediante la clase *MultiValueChangeAwareSource*.

Los datos recogidos antes de ser redirigidos hacia las capas superiores deben ser adecuados a los formatos aceptados por la SCMF para el almacenamiento en su base de datos. La clase *Mapper* permite a partir de una instancia de un objeto generar otro que se adecue a los requerimientos de la SCMF.

En la figura 6.33 se muestra un ejemplo de la implementación del recolector de batería empleando la estructura descrita. Mediante configuraciones basadas en XML se define el comportamiento del recolector y qué clases son las que se encargan de realizar las tareas. Así por ejemplo, modificando el *Mapper* o traductor asociado se podrían cambiar fácilmente las unidades para definir el nivel de batería o establecer un nivel porcentual.

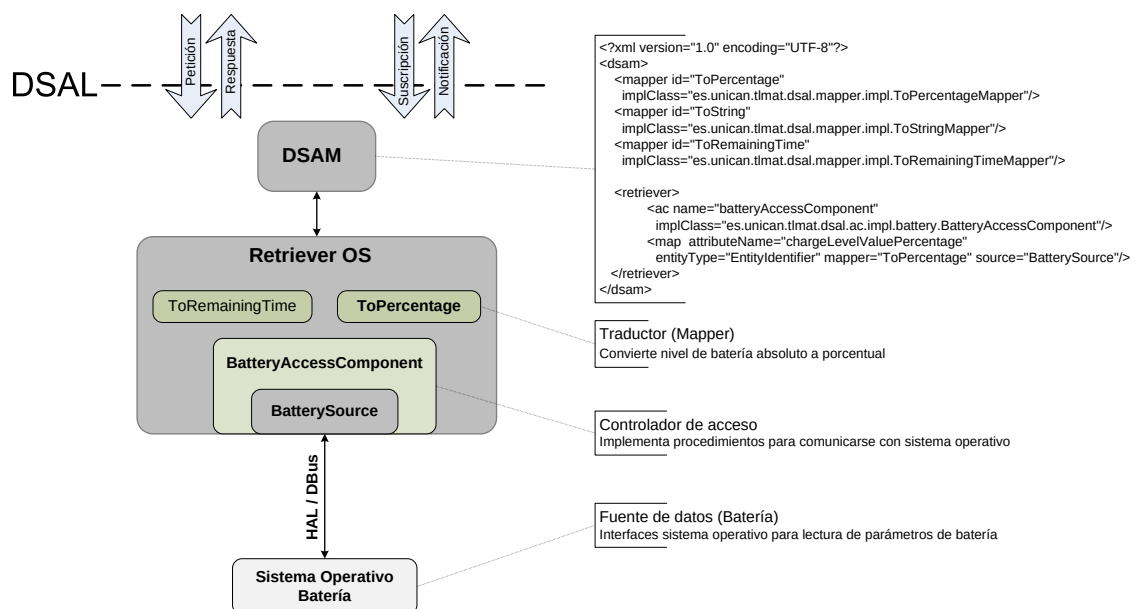


Figura 6.33: Detalle de la implementación del recolector de datos de batería

A continuación se describen los trabajos realizados sobre el recolector de datos del sistema

operativo y de la UCL. La información recogida será usada como entrada a la función de coste de la implementación del protocolo anteriormente descrito.

6.3.3.1. Recolector del sistema operativo

Gran parte de la información de contexto de un nodo no reside en el entorno de dicho nodo sino en él mismo. El sistema operativo es la única puerta de la que disponen los usuarios hacia múltiples parámetros tanto *software* como *hardware*. De ahí que desde la comunidad de desarrolladores se ponga tanto empeño en tratar de proporcionar unas interfaces amigables y homogéneas para acceder a esa información.

Desktop Bus (D-Bus) [214] es un sistema de comunicación entre procesos (IPC, *Inter-Process Communication*) para que aplicaciones de *software* puedan comunicarse entre sí. Originalmente desarrollado como parte del proyecto *freedesktop.org* para el sistema operativo Linux (actualmente se encuentra disponible para otros sistemas operativos), intenta unificar las múltiples alternativas de IPC en un único protocolo. Su diseño busca permitir el intercambio de datos entre procesos de sistema y de usuario.

Teniendo en cuenta las características expuestas, D-Bus puede considerarse como la opción más apropiada para recoger información interactuando con el sistema operativo. La API de bajo nivel y el protocolo de transferencia binaria de mensajes permiten la comunicación entre procesos de un mismo equipo empleando una baja latencia y la mínima sobrecarga. La comunicación generalmente suele seguir una metodología centralizada, concentrando los mensajes en un servidor, conocido como *bus*, pero también permite la comunicación directa entre los procesos.

Por otro lado, los sistemas operativos actuales funcionan sobre muy diversas plataformas *hardware*. Buscando ocultar las diferencias en el *hardware* al entorno *software*, surge la capa de abstracción de *hardware* (HAL, *Hardware Abstraction Layer*) de forma que el *kernel* no deberá modificarse para ejecutarse en diferentes *hardwares*. HAL puede considerarse un *driver* genérico de la placa base de los dispositivos que proporciona acceso a la información a través de D-Bus de forma síncrona o asíncrona. HAL considera cada parte del *hardware* como un objeto identificado de forma única y cuyas propiedades se representan mediante una dupla de identificador-valor. En la especificación se puede encontrar la definición de múltiples propiedades [215].

La representación empleada por HAL tiene muchas similitudes con la utilizada dentro de la SCMF, puesto que una entidad a nivel SCMF se puede relacionar directamente con un objeto HAL y los atributos serán las propiedades del objeto. Adicionalmente, ambas plataformas comparten la identificación única de los objetos o entidades, con la diferencia de que HAL sólo considera el entorno del nodo local. Para conseguir un identificador global, el identificador de la entidad a nivel SCMF se genera concatenando el identificador del nodo y el del objeto.

El análisis de la información que es posible recolectar a través de HAL revela que la mayoría de los tipos de datos asignados son los considerados nativos, es decir, enteros (*int*, *long*, etc.), booleanos, cadenas de caracteres (*string*), etc.

Por tanto, adaptar las descripciones de HAL a las de la ontología adoptada en la SCMF resulta sencilla. Los recolectores del sistema operativo generados emplean la metodología de

señalización proporcionada por D-Bus, lo que supone que la SCMF obtendrá notificaciones instantáneas ante cualquier cambio en las propiedades del dispositivo.

En base a lo explicado y tal como se observa en la figura 6.33, se ha implementado un recolector de información relacionada con el estado energético del dispositivo (batería, cargador, etc.). También se ha desarrollado otro recolector de información propia del dispositivo, como la identidad, tipo de *hardware*, memoria disponible, versión del sistema, etc. con la que poblar los atributos de la entidad *Computer*. Estas nuevas entidades, mostradas en la figura 6.34, se han definido e implementado siguiendo las reglas impuestas por la ontología del proyecto MAGNET [135], que a su vez ha sido actualizada para incluirlas.

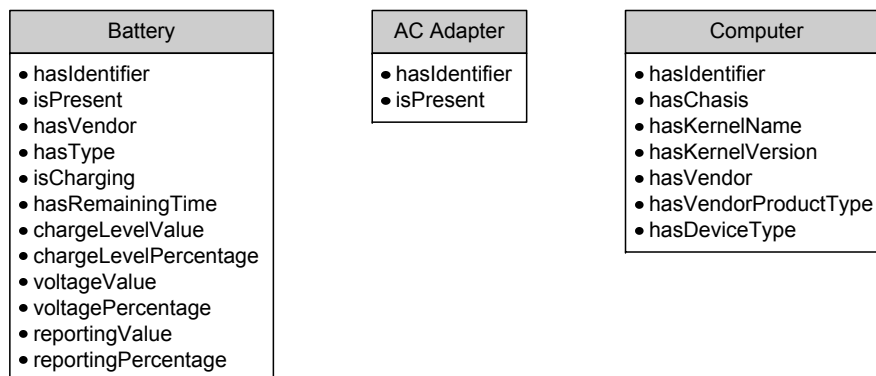


Figura 6.34: Entidades asociadas al sistema operativo

El significado de los atributos se explica por sí mismo a partir del nombre, aunque más detalle puede encontrarse en la especificación HAL.

La información recogida mediante estos recolectores puede ser accesible bien a través de suscripción o de solicitud directa. Algunos parámetros, principalmente los relacionados con la entidad *Computer*, no suelen cambiar a lo largo de la vida de un dispositivo, por lo que es más adecuado realizar una única petición al inicio. Sin embargo, atributos como niveles de batería (*chargeLevelValue*), el tiempo restante de autonomía (*hasRemainingTime*) o la presencia del cargador (*isPresent*) varían con frecuencia. Es recomendable usar la suscripción y notificación asíncrona para actualizar los valores de estos atributos.

6.3.3.2. Recolector de la UCL

La implementación de la UCL, como se describe en el apartado 6.2.1, combina programas de espacio de usuario con módulos del *kernel*. A pesar de que los módulos del *kernel* incluyen gran variedad de mecanismos para interactuar con el espacio de usuario de forma estándar, el conjunto de utilidades de espacio de usuario reformula alguno de ellos para hacer más accesibles las capacidades e información de la UCL.

En este sentido, la UCL implementa la notificación de cambios en el estado de los vecinos y en el canal al espacio de usuario a través de *Netlink sockets*. Puesto que D-Bus ofrece una metodología simple y genérica para el intercambio de información entre aplicaciones y dado que el recolector del sistema operativo ya desarrollado incluye un adaptador de objetos D-Bus a entidades descritas según la ontología de MAGNET, se decidió implementar una

utilidad de espacio de usuario que a partir de los mensajes *Netlink* generara objetos D-Bus. Posteriormente, haciendo uso del adaptador de la SCMF, se estableció la conexión entre la UCL y la SCMF, habilitando tanto el mecanismo de suscripción-notificación como el de solicitud-respuesta a través del lenguaje CALA.

De esta forma se logra exportar la información asociada a la estructura del *cluster*, vecinos de un nodo y estadísticas relacionadas con ellos. La figura 6.35 presenta las nuevas entidades que se han añadido a la ontología existente. Las instancias de estas entidades se generan de forma automática según vayan surgiendo nuevos nodos. Así, como ejemplo de uso, se recomienda suscribirse a cambios en atributos como `hasConnectedNode` para conocer la aparición o desaparición de nuevos nodos en el *cluster*.

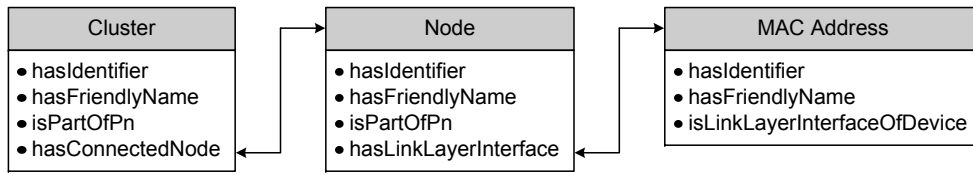


Figura 6.35: Entidades asociadas a la estructura de red

Disponer de un recolector de información de la UCL y exportar estos datos a la SCMF permite obtener información de nodos remotos sin tener que demandársela a ellos. Además de la notable reducción de la sobrecarga de red, el procedimiento basado en suscripción/-notificación dota de instantaneidad a la actualización de las métricas, al tiempo que reduce el consumo de energía en el que se incurre con el sondeo periódico.

6.3.4. Evaluación

A continuación se detalla el proceso de evaluación del procedimiento diseñado. En primer lugar se plantea un estudio simulado que permita conocer el rango a partir del cual ajustar los temporizadores. Posteriormente, empleando estos valores, se implementa e integra el protocolo tanto en la SCMF como en la SMP.

6.3.4.1. Simulación

Como paso previo a la implementación, se requiere determinar la relación entre los temporizadores de negociación y estabilización. Para ello se simuló el procedimiento en el simulador *Network Simulator v2* (NS-2) [216] con el propósito de analizar el comportamiento del *cluster* en función del parámetro m . Para el ajuste de dicho valor se define como métrica el número de nodos candidatos cuyo temporizador de estabilización expira antes de recibir el primer anuncio del nuevo gestor. A medida que el valor de m se incrementa es de esperar que el número de nodos con fallos del temporizador se reduzca.

La figura 6.36 muestra los resultados de las simulaciones realizadas para escenarios con 5, 10 y 30 nodos dispuestos de forma aleatoria, considerando diferentes distancias entre ellos.

Tal como cabía esperar las simulaciones reflejan cómo el número de fallos decrece al aumentar el parámetro m , siendo a partir de 1 cuando se observa una estabilización, llegando a situaciones sin fallos. Considerando el escenario de 5 nodos, que simula un *cluster* pequeño,

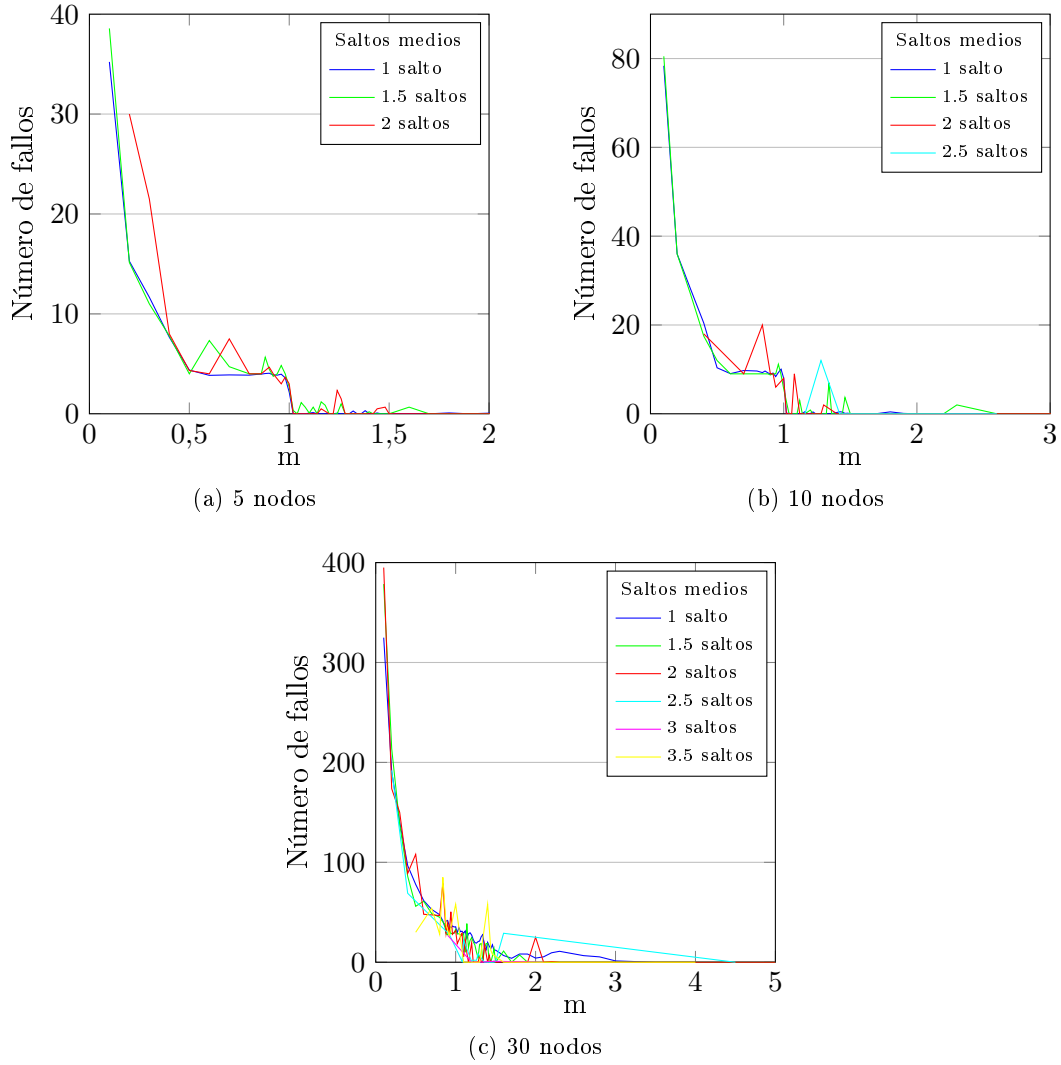


Figura 6.36: Evaluación del proceso de selección de gestor

para valores de m entre 1,02 y 1,05 no se incurre en fallos. Para *clusters* de 10 nodos se mantiene aproximadamente el rango de m , si bien se observa que un número medio de saltos entre los nodos mayor que hace se requieran valores de m superiores (aproximadamente 1,15). En los escenarios de 5 nodos es más difícil analizar situaciones de multisalto.

Para completar el estudio se simuló un escenario con 30 nodos como planteamiento de *clusters* personales en el hogar o la oficina. Los valores obtenidos mantienen la tendencia observada en los escenarios anteriores al aumentar el número medio de saltos, en este caso con valores de m entre 1,1 y 1,4. No obstante, hay que destacar los resultados obtenidos para el escenario donde los nodos se encuentran a un único salto. En esta situación el valor óptimo de m se eleva por encima de 1,5. Se considera que la causa de este comportamiento es el elevado número de colisiones causadas por el envío de mensajes de difusión y retransmisiones entre los nodos. En los escenarios en los que los nodos están distribuidos en un área mayor,

el número de vecinos de cada uno es menor y se retransmite un menor número de paquetes, lo que incide en menos colisiones.

Los valores obtenidos de las simulaciones se consideran el límite inferior, por lo que se recomienda que en la implementación en entornos reales se incremente m en un pequeño porcentaje.

6.3.4.2. Integración en SCMF y SMP

Seguidamente se describen los detalles de la prueba de concepto realizada integrando el procedimiento definido tanto en la SCMF como en la SMP y el resultado obtenido de ellas. El desarrollo *software* del protocolo se ha realizado en lenguaje Java para mantener la homogeneidad con el lenguaje empleado en las plataformas de servicio y contexto.

El primer paso en la implementación es ajustar el comportamiento de la función de coste. Se ha optado por otorgar un peso del 70 % (ω_R) a los recursos del nodo, siendo el restante 30 % asignado a la conectividad (ω_C), normalizando los valores de ambos pesos a un valor máximo de 100. Así, por ejemplo, se define el valor máximo de $C(v)$ cuando el número de vecinos supera los 5, con una calidad de enlace equivalente a emplear interfaces IEEE 802.11a en condiciones ideales. Por su parte, en el cálculo de $R(v)$ se otorga un factor preferencial a las capacidades energéticas y de cómputo, puesto que, además de que $C(v)$ de cierta forma está ligado al número de interfaces de red disponibles, se busca la estabilidad en el papel del gestor para no tener que incurrir en constantes cambios de contexto. $L(v)$ se referencia como la media de la carga de cada uno de los procesadores de que disponga el terminal. En este sentido, el valor actual se incrementa para considerar la variación de carga que deberá soportar el nodo al realizar las tareas de gestor. No obstante, las pruebas resultantes revelaron que el porcentaje era prácticamente despreciable debido a que los nodos candidatos ya ejecutan la mayoría de las funcionalidades de la SCMF y/o SMP.

Las pruebas realizadas validaron el procedimiento definido [123], pues independientemente del momento en el que se iniciaran los nodos y el estado de cada uno de ellos siempre se lograba seleccionar un único gestor. El protocolo de encaminamiento permitió la transmisión de las primitivas a todos los nodos del *cluster*, lo que posibilitó la validación de los procesos de fusión y separación.

Como ya se ha mostrado, la figura 6.31 presenta el diagrama temporal de uno de los experimentos realizados y que sirve para comprender mejor el funcionamiento del procedimiento de selección. Durante las pruebas, el tiempo entre mensajes de anuncio se fijó a 5 segundos dado que se trataban de experimentos donde se forzaban rápidos cambios en el escenario. Sin embargo, este tiempo podría ajustarse en función del peso del nodo gestor, de forma que a medida que este valor se aproximase más al nivel de traspaso, el tiempo entre anuncios se redujera, buscando predisponer a otros nodos a tomar la responsabilidad.

De las pruebas se concluyó que un valor adecuado como límite para disparar el proceso de búsqueda ante la no detección de la presencia de un gestor es 1,5 veces el tiempo entre mensajes de anuncio fijado para el gestor. Por otro lado, la implementación también consideró que en el caso de que un gestor renuncie al puesto pero no haya ningún candidato con mejores capacidades, restaurar el estado previo conllevaría aproximadamente 2 veces el tiempo entre anuncios.

6.4. Movilidad en la PN

La arquitectura de red planteada en el capítulo 3, donde se da soporte a la PN a través de una red virtual, permite la gestión del tráfico tanto intra-*cluster* como inter-*cluster*. Dentro de un *cluster* la comunicación se establece haciendo uso de protocolos de encaminamiento ad-hoc multisalto y de las capacidades de la UCL, que permite la interconexión de varios DR, mientras que las comunicaciones entre nodos de *clusters* diferentes hacen uso del concepto de túneles dinámicos gestionados por los nodos pasarela de cada *cluster* en coordinación con el agente de la PN.

Algo tan importante como la movilidad de los nodos personales también se ha tenido en cuenta en las soluciones propuestas. La movilidad dentro de un mismo *cluster* está inherentemente resuelta con el encaminamiento ad-hoc. Por su parte, cuando un nodo se mueve de un *cluster* a otro, los nodos pasarela involucrados remiten la información del cambio al agente de la PN para que éste informe al resto de los *clusters* de la nueva ruta hacia ese nodo. Del mismo modo, cuando un nodo pasarela, como representante de un *cluster*, cambia su punto de contacto, informa al agente de la PN de su nueva localización y restablece los túneles seguros de comunicación con el resto de los *clusters*. En este sentido, se puede apreciar que la especificación de la PN considera tanto la movilidad de las agrupaciones de nodos de usuario, como la de sus componentes.

En la definición de los mecanismos de comunicación dentro del proyecto MAGNET, principalmente aquellos enfocados a la interconexión de *clusters*, también se buscó dar respuesta no sólo a la comunicación entre los nodos, sino que se incluyeron aspectos que permitieran el reúso de parte de los componentes para otros propósitos, como puede ser el contexto o el descubrimiento y provisión de servicios. Un ejemplo claro de esta filosofía es el agente de la PN, que aglutina funcionalidades para dar soporte a la comunicación entre nodos o a la movilidad y que colabora en el descubrimiento de servicios y en su provisión.

La adopción de esta metodología de operación no seguía procedimientos estándares. No obstante, las discusiones mantenidas durante el proyecto [217] plantearon también opciones para dar soporte a la comunicación y movilidad de los nodos usando estándares como MIP [15, 16], enfocado más a dar soporte a la movilidad de nodos, o NEMO [17], extensión de MIPv6 que da soporte a agrupaciones de nodos.

La implementación y despliegue de pilotos de la PN y la PN-F, tal como se ha descrito, se realizaron con unos resultados satisfactorios [186]. De la colaboración en estos pilotos y del conocimiento adquirido en la integración de los diferentes componentes, unido a la estabilización de los estándares y la disponibilidad de implementaciones básicas en las que apoyar los desarrollos, surge el interés en analizar las opciones descartadas. Así, como parte del trabajo de investigación llevado a cabo en esta tesis, se realiza el análisis y despliegue de una red basada en MIP que emule el comportamiento de los nodos de la PN en movilidad.

A continuación se expone la labor realizada para evaluar la viabilidad de MIPv6 para gestionar el traspaso de un nodo o de un *cluster* completo de una localización a otra en un entorno multi-interfaz radio. En [218] se incluye un estudio preliminar de diferentes soluciones de soporte *multihoming* que guió este despliegue. El escenario supuesto, resuelto ya con soluciones propietarias, consiste en un nodo pasarela, representante de un *cluster* personal, que en movilidad se vincula a diferentes puntos de interconexión a la infraestructura de red.

6.4.1. Arquitectura de la PN adaptada a MIPv6

Las arquitecturas de movilidad especificadas en MAGNET y en MIPv6 tienen grandes similitudes que permiten establecer una correspondencia prácticamente directa entre las entidades, lo que facilitará la comparativa entre la operativa de ambas.

En MIPv6 la gestión de movilidad se realiza en base a tres elementos: el nodo móvil (MN, *Mobile Node*), el HA y el nodo correspondencial (CN, *Correspondent Node*). El MN y el CN representan los extremos de la comunicación, mientras que el HA es la entidad que mantiene la asociación entre la dirección del MN en su red de origen *Home Address* (HoA) y la asignada en movilidad *Care-of Address* (CoA) y habilita la comunicación transparente entre el MN y el CN. MIPv6 actúa directamente sobre la capa de red como extensión a IPv6. La transferencia de información entre el MN en itinerancia y su HA se establece mediante un túnel IPsec que protege la integridad y autentica la comunicación.

A la vista de lo anterior, las figuras del MN y del CN se reflejan en cualquier nodo personal y externo, mientras que las competencias del HA encajan con las definidas para el agente de la PN. El procedimiento más común para desplegar MIPv6 supone que el HA hace las veces de pasarela entre el MN y el CN. Esta operativa difiere de la especificada en MAGNET, pues una vez establecidos los túneles la comunicación se realiza de forma directa entre ellos. No obstante, MIPv6 incorpora el mecanismo *Return Routability Procedure* (RRP) que habilita la comunicación directa entre el MN y el CN. Dado que esto supone incluir modificaciones en el CN, nodo que puede no pertenecer a la PN, se ha preferido mantener la configuración más usual de MIPv6 para dotar de mayor generalidad a las pruebas.

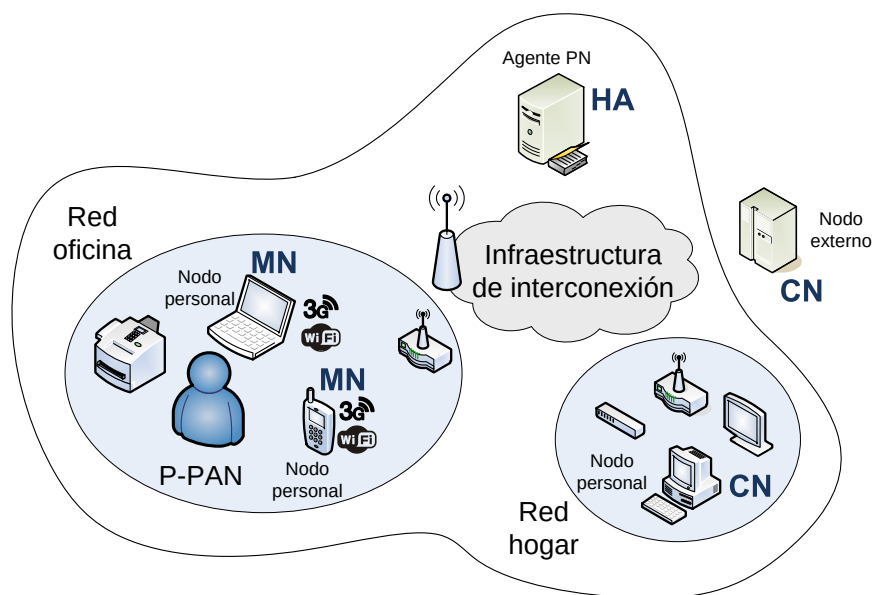


Figura 6.37: Arquitectura de MIPv6 sobre MAGNET

El escenario de experimentación, cuyo esquema lógico se muestra en la figura 6.37, contempla un nodo personal con varias interfaces de comunicaciones inalámbricas. Se dispone que el nodo podrá establecer conexiones de datos a través de redes IEEE 802.11abgn y GPRS/UMTS. Este nodo realizará el desplazamiento de una red IEEE 802.11abgn hacia

una red móvil GPRS/UMTS en ambos sentidos mientras accede a un servicio de difusión de vídeo provisto por el nodo externo. Buscando la generalidad, se ha optado por usar un nodo externo como CN, ya que usar únicamente la red propia de la PN se presenta como una opción menos restrictiva.

El traspaso entre redes se puede realizar de dos formas, de forma automática o guiado por el usuario. Es bien sabido que el escaneo continuo para la búsqueda de redes disponibles en el entorno del usuario, especialmente en las basadas en IEEE 802.11, y la conexión automática implican un elevado consumo de batería. Con esta técnica además no se garantiza que la red a la que el terminal se conecte cumpla con los requerimientos de conectividad y soporte de movilidad establecidos. En este sentido, para facilitar la experiencia de uso, se ha optado por controlar el traspaso entre redes mediante el uso de la tecnología NFC. De esta forma será el usuario quien, aproximando su terminal a una etiqueta NFC con la información de la red objetivo, inicie el traspaso. Así, además de conseguir mejorar la durabilidad de la batería al poder tener apagada la interfaz hasta que se produzca la lectura de la etiqueta y se inicie el traspaso, también se garantiza que la red a la que el usuario se conecta soporta los requerimientos y necesidades establecidos en términos de gestión de la movilidad. La inclusión de este modo de gestionar el traspaso permitirá también evaluar la experiencia de uso de la nueva tecnología NFC y probar nuevos casos de uso de ella más allá del tradicional entorno de pago y control de accesos.

6.4.2. Plataforma de experimentación

6.4.2.1. *Hardware* empleado

Aunque en las primeras fases del desarrollo se realizaron sobre ordenadores portátiles, las configuraciones e implementaciones se migraron a equipos de uso cotidiano y más acordes con los que se plantean dentro de una PN. A continuación se describen brevemente dichos dispositivos.

6.4.2.1.1. *Routers* basados en ALIX 2D13

Las placas ALIX 2D13 [219] fabricadas por PC Engines embeben en un mismo sistema un procesador AMD Geode LX800 con 256 MB de memoria *Random Access Memory* (RAM) y tres interfaces de comunicaciones Ethernet. Dispone de dos puertos de *Universal Serial Bus* (USB), bus *Integrated Device Electronics* (IDE) y ranura mini-PCI de expansión.

Se ha empleado este *hardware* para implementar la infraestructura de red. Para ello se han añadido al *hardware* básico una tarjeta inalámbrica Compex WLM54AG y un módem USB *High-Speed Downlink Packet Access* (HSDPA) Huawei E220.

De entre los múltiples sistemas operativos soportados (OpenWRT [220], CentOS, Ubuntu, etc.) se ha optado por configurar las placas con Voyage Linux [221], una distribución basada en Debian Sarge especialmente diseñada para funcionar en plataformas embebidas basadas en arquitecturas x86 como ALIX.

6.4.2.1.2. Teléfono inteligente Google Nexus S

El teléfono móvil Google Nexus S [222] es el segundo teléfono inteligente puesto en el

mercado bajo el control directo de Google. Fabricado por Samsung, está equipado con un procesador ARM Cortex A8 a 1 Ghz y 512 MB de memoria RAM. Dispone de interfaces de comunicaciones HSDPA a 7.2 Mbps, IEEE 802.11n, Bluetooth 2.1 y NFC. De fábrica incorpora la versión 2.3.4 del sistema operativo Android, si bien ésta se puede personalizar y actualizar posteriormente.

6.4.2.2. Implementaciones MIPv6 en Linux

Existen varias implementaciones de MIPv6 para Linux pero, en el momento de realizar este trabajo, la mayoría estaban desactualizadas o habían quedado obsoletas. Un claro ejemplo es el caso de *Mobile IPv6 for Linux v2.0* (MIPL2), el cual estuvo constituido en su momento por un conjunto de parches que implementaban el RFC 3775 [223]. Esta implementación era únicamente válida para la versión 2.6.16 del *kernel* de Linux y actualmente se encuentra totalmente desactualizada y la evolución del proyecto parece abandonada.

Tomando como base el código de MIPL2, un grupo de desarrolladores del proyecto *Universal playGround for Ipv6* (USAGI) crearon *Universal MIP* (UMIP) [224] con soporte para *kernels* de Linux más modernos. Esta versión soporta no sólo el estándar RFC 3775 [223] sino también el RFC 3776 [225]. Con más actividad que la anterior, existe un *fork* del proyecto, UMIP.org [226] que simplifica la codificación y configuración al tiempo que añade soporte para NEMO. Ésta será la versión que se utilice para evaluar MIPv6 en entornos personales.

La implementación de MIPv6 seleccionada requiere que funcionalidades tanto en el espacio de ejecución de *kernel* como en el de usuario operen conjuntamente. Por un lado, el *kernel* de Linux de la máquina debe tener habilitado el soporte de movilidad MIPv6, opción que normalmente no está activada por defecto, lo que implica tener que recompilar el *kernel*. Las opciones mínimas de configuración a añadir se muestran en el cuadro de texto 6.7.

Mientras en el espacio de *kernel* se da soporte a los protocolos de comunicaciones, en el espacio de usuario, por su lado, el demonio *mip6d* implementa las funcionalidades de gestión del entorno MIPv6, haciendo que un equipo adopte, según la configuración, el rol de MN, HA o CN. Este demonio además crea una nueva interfaz virtual que encapsula las interfaces reales que participen del ecosistema MIPv6. Será sobre esta interfaz sobre la que se construya el túnel IPv6-over-IPv6 entre el MN y el HA y tendrá asignada una dirección perteneciente a la red de origen.

6.4.3. Despliegue realizado

Descritos brevemente los componentes principales, se detalla a continuación la implementación del soporte a la movilidad en una red personal empleando MIPv6. Se divide la explicación en dos partes: primeramente el establecimiento y configuración de la capa de red con soporte MIPv6, para posteriormente afrontar en la gestión del traspaso por parte del usuario.

6.4.3.1. Soporte MIPv6 a nivel de red

Antes de poder ejecutar los protocolos de movilidad basados en MIPv6 es necesario configurar las entidades que forman parte del entorno de pruebas (*routers* y máquinas

Cuadro de texto 6.7: Opciones de configuración del *kernel* de Linux para soportar MIPv6

```

General setup
--> Prompt for development and/or incomplete code/drivers [CONFIG_EXPERIMENTAL]
--> System V IPC [CONFIG_SYSVIPC]

Networking support [CONFIG_NET]
--> Networking options
--> Transformation user configuration interface [CONFIG_XFRM_USER]
--> Transformation sub policy support [CONFIG_XFRM_SUB_POLICY]
--> Transformation migrate database [CONFIG_XFRM_MIGRATE]
--> PF_KEY sockets [CONFIG_NET_KEY]
--> PF_KEY MIGRATE [CONFIG_NET_KEY_MIGRATE]
--> TCP/IP networking [CONFIG_INET]
--> The IPv6 protocol [CONFIG_IPV6]
--> IPv6: AH transformation [CONFIG_INET6_AH]
--> IPv6: ESP transformation [CONFIG_INET6_ESP]
--> IPv6: IPComp transformation [CONFIG_INET6_IPCOMP]
--> IPv6: Mobility [CONFIG_IPV6_MIP6]
--> IPv6: IPsec transport mode [CONFIG_INET6_XFRM_MODE_TRANSPORT]
--> IPv6: IPsec tunnel mode [CONFIG_INET6_XFRM_MODE_TUNNEL]
--> IPv6: MIPv6 route optimization mode [CONFIG_INET6_XFRM_MODE_ROUTEOPTIMIZATION]
--> IPv6: IPv6-in-IPv6 tunnel [CONFIG_IPV6_TUNNEL]
--> IPv6: Multiple Routing Tables [CONFIG_IPV6_MULTIPLE_TABLES]
--> IPv6: source address based routing [CONFIG_IPV6_SUBTREES]

File systems
--> Pseudo filesystems
--> /proc file system support [CONFIG_PROC_FS]

```

Linux) para que exista una conectividad a nivel de red entre todas ellas. Esto implica que se deberán fijar las rutas necesarias de tal forma que los nodos se reconozcan entre sí. Para ello, se puede adoptar una estrategia dinámica o estática. La configuración dinámica permite establecer rutas de forma automática mediante el uso de demonios de encaminamiento tales como Quagga[227]. Caso contrario se tendrían que configurar las rutas de forma manual. Aunque la configuración estática aparenta estar en desventaja frente a la dinámica, permite tener un mayor control sobre el comportamiento de la red. La asignación de direcciones en la PN, aunque dinámica, es controlada por el agente de la PN y los nodos mantienen la dirección a lo largo de su ciclo de vida. Por estas razones, para estas pruebas se ha optado por una configuración estática, estableciéndose las rutas según se muestra en la figura 6.38. Debido a que los operadores de red móvil actualmente no soportan IPv6 en sus redes de forma nativa, se hace necesario encapsular el tráfico IPv6 sobre IPv4 mediante el uso de túneles. La figura 6.39 muestra gráficamente este comportamiento.

Los equipos embebidos ALIX se han dispuesto para que hagan las labores de *routers* inalámbricos IEEE 802.11 y GPRS/UMTS. Para el primero de los casos, se configura *hostap* [228] para habilitar la funcionalidad de punto de acceso y *radvd* [229] para el anuncio de las rutas IPv6 mediante el método de autoconfiguración sin estado (*stateless autoconfiguration*). De esta forma el MN adquiere una dirección IPv6 en la red y configura su tabla de rutas adecuadamente. Para el caso GPRS/UMTS la configuración se reduce a disponer el programa *wvdial* [230] para establecer una conexión a través del módem empleando el protocolo punto a punto (PPP, *Point-to-Point Protocol*).

Teniendo conectividad sobre la infraestructura de red dispuesta, resta configurar MIPv6 para que opere sobre ella. Tanto el MN como el HA ejecutarán el demonio de control *mip6d*, señalando en su configuración las interfaces de red que deberá gestionar. Para el MN se plantea, como se ha indicado ya, el uso de interfaces IEEE 802.11 e GPRS/UMTS,

6. VALIDACIÓN EXPERIMENTAL

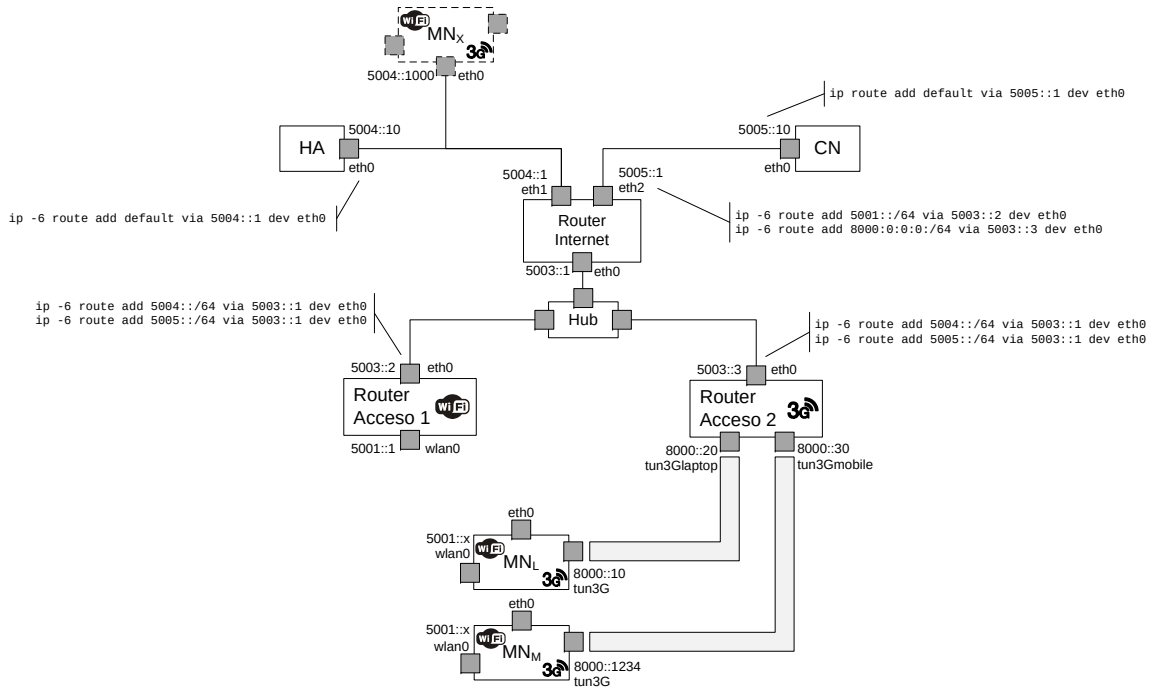


Figura 6.38: Configuración global de red del entorno de pruebas MIPv6

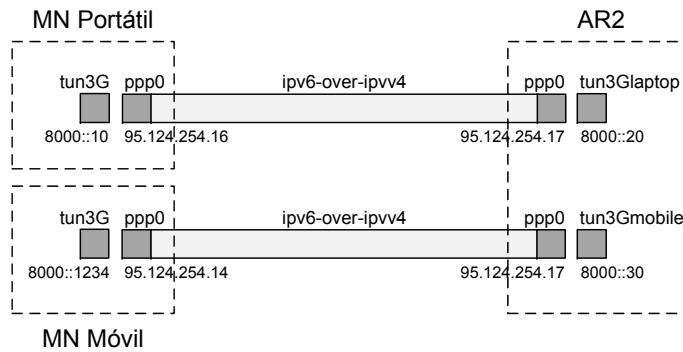


Figura 6.39: Visión de los canales de comunicación del entorno de pruebas sin MIPv6

otorgando, por defecto, preferencia de uso a la interfaz IEEE 802.11. Esto significa que si ambas interfaces están activas al mismo tiempo y pueden mantener una conexión, la comunicación se realizará mediante la interfaz IEEE 802.11. En caso que la interfaz IEEE 802.11 no tenga conectividad, se empleará la interfaz de banda ancha. Este comportamiento inherente al demonio `mip6d` se asemeja, aunque con menos posibilidades, a la gestión multi-interfaz que se realiza con la UCL.

El nodo CN es el extremo de la conexión que actúa como proveedor del servicio. Dicho nodo no se modifica, sino que opera como un nodo tradicional, no incluyendo las mejoras para la optimización de rutas disponibles en MIPv6.

En la figura 6.40 se presenta el detalle de la incorporación de MIPv6 al sistema. La

comunicación entre el MN y su correspondiente HA se realiza encapsulada en un túnel IPv6-sobre-IPv6.

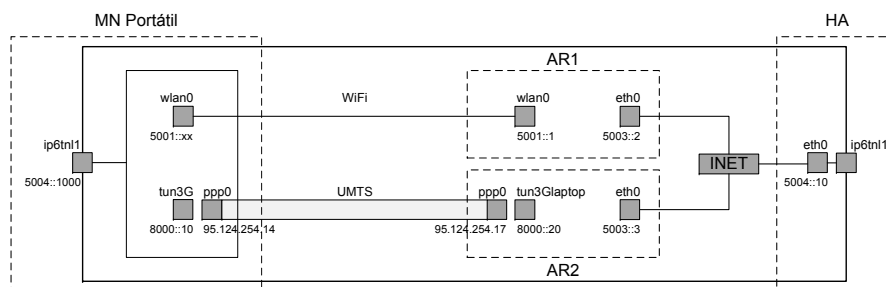


Figura 6.40: Canales de comunicación del entorno de pruebas con MIPv6 habilitado usando un equipo portátil

Hasta este punto todas las configuraciones y pruebas realizadas para determinar la estabilidad del sistema se llevaron a cabo empleando como MN un equipo portátil con suficiente potencia y una gran flexibilidad de configuración. Ahora bien, la PN está compuesta por un conjunto diverso de dispositivos y se hace necesario experimentar con tabletas y/o teléfonos móviles. A pesar de seleccionar uno de los terminales más versátiles del mercado como el Google Nexus S, se detectaron diversas limitaciones que provocaron la modificación de la configuración realizada para los portátiles.

Aunque el sistema operativo Android implementa soporte para IPv6 y se puede configurar el soporte MIPv6 sobre una plataforma basada en la arquitectura ARM [231] (los detalles de la implementación se pueden encontrar en [218, 232, 233]), la mayor parte de las aplicaciones para Android, especialmente las de visionado de difusión de audio/vídeo, no soportan el direccionamiento IPv6. Por tanto, aun estando el entorno de comunicaciones MIPv6 subyacente operativo, éste no se podía usar de forma nativa.

Los servicios multimedia son posiblemente los servicios más demandados por los usuarios, por lo que la validación de la solución de movilidad MIPv6 sobre terminales móviles supone obligatoriamente soportarlos. Además, desde el punto de vista de evaluación del rendimiento de la red y del traspaso, ofrecen un escenario con unas características especiales en cuanto a requerimientos de canal, variabilidad de la tasa de tráfico, etc. Por estas razones se buscaron alternativas que permitieran solventar el problema.

La solución natural consistió en superponer un nuevo túnel extremo a extremo entre el MN y el CN, que emulara la comunicación IPv6 entre el cliente y el servidor sobre un canal IPv4. La figura 6.41 actualiza la configuración presentada en la figura 6.40, incluyendo este nuevo túnel. Aunque esta medida pueda afectar al rendimiento, se consideró la solución menos invasiva.

6.4.3.2. Gestión del traspaso mediante NFC

El traspaso de la comunicación entre redes planteado incorpora el uso de la tecnología NFC como método de disparo. Se considera que la lectura de una etiqueta NFC permite adquirir la información necesaria para establecer la conexión con una red inalámbrica de confianza. El formato definido para almacenar esta información se presenta en la figura 6.42.

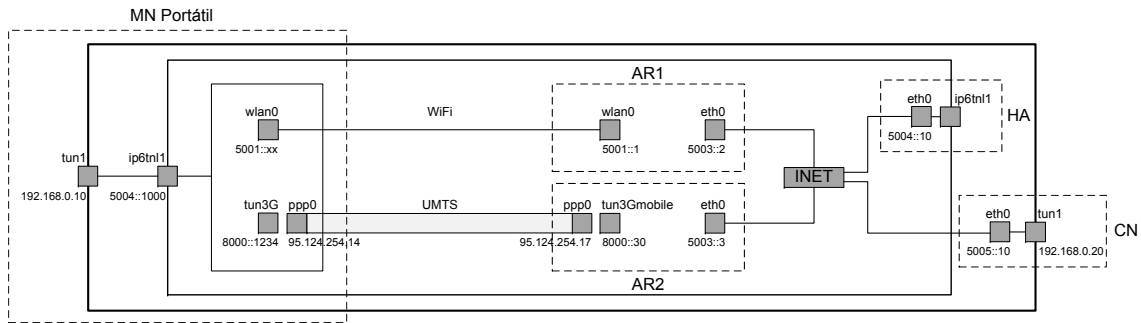


Figura 6.41: Canales de comunicación del entorno de pruebas con MIPv6 habilitado usando un cliente móvil

1	1	1	1	1	1	n	n
Visibilidad	Algoritmos autenticación	Cifrado de grupo	Esquemas gestión claves	Cifrado entre pares WPA	Protocolos de seguridad	SSID	Claves

Figura 6.42: Formato de la información en la etiqueta NFC

Siguiendo las recomendaciones del *NFC Forum* [234], los datos se graban en la etiqueta en un registro *NFC Data Exchange Format* (NDEF) de tipo *TNF_MIME_MEDIA* propio, para el cual se ha definido *application/wifitag.unican.es* como el tipo *Multipurpose Internet Mail Extensions* (MIME) [235-239]. El hecho de definir este tipo para el registro NDEF permite un sencillo filtrado de la lectura de etiquetas, de tal forma que se pueda configurar el aplicativo para que sólo responda a lecturas de etiquetas con este tipo de registro. Más estándar hubiera sido emplear un registro de tipo *External*, pero no está soportado en la versión 2.3.4 de Android, plataforma sobre la que se ha desarrollado el aplicativo; a pesar de ello, la funcionalidad lograda es similar.

El aplicativo móvil, cuya interfaz se describe a continuación, implementa también la grabación de etiquetas con este formato a partir de las redes inalámbricas disponibles en el entorno del usuario.

6.4.3.3. Interfaz de usuario

Una vez que se ha especificado todo el proceso de configuración de los diferentes elementos de la red, tanto *routers* como terminales móviles, seguidamente se procede a describir la aplicación de usuario que, instalada en su teléfono, le permitirá hacer uso de las funcionalidades de movilidad planteadas. Dicha aplicación, desarrollada específicamente para teléfonos Android, incorpora las siguientes funcionalidades:

- Gestión del entorno de movilidad MIPv6.
- Visualización de vídeo con control de estado de descarga.
- Reproducción de audio con visualización de estado de descarga.
- Activación/selección del interfaz de red de transmisión.

- Soporte para lectura y escritura de etiquetas NFC con información de redes inalámbricas.

En la figura 6.43 se muestra la captura de pantalla del interfaz de usuario. Puesto que se trata de una prueba de concepto, la interfaz de usuario es austera y simple, orientada a permitir visualizar la información necesaria dentro del entorno de pruebas. La parte superior presenta el control del flujo de audio, mientras que en la inferior se realiza la visualización del vídeo. La parte central se ha reservado para la administración de las comunicaciones y gestión de la movilidad.

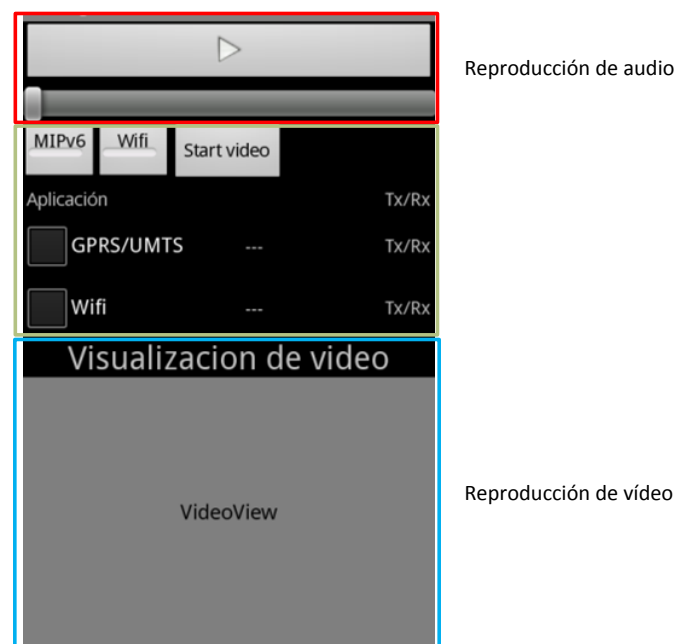


Figura 6.43: Interfaz de usuario en teléfono móvil

La ejecución de la aplicación requiere que el teléfono tenga habilitado el modo de ejecución con permisos de administración, pues accede a las configuraciones de red y las modifica. En este sentido, en la primera ejecución es recomendable guardar las preferencias de ejecución para facilitar la experiencia de uso.

Al iniciar el aplicativo, en la parte central aparecerá la información de las interfaces inalámbricas disponibles. Considerando que la interfaz IEEE 802.11 se encuentra deshabilitada, se presenta únicamente la información de la interfaz móvil, indicando el tipo de conexión, operador empleado y el tráfico generado tanto de subida como de bajada desde el inicio de la aplicación.

Por defecto el entorno de movilidad se encuentra deshabilitado, por lo que al tratar de visualizar algún vídeo o reproducir el audio, se producirá un error al no tener conectividad con el servidor. Para habilitar el soporte MIPv6 se debe pulsar sobre el botón MIPv6 y, si todo el proceso de iniciación y registro se realiza de forma satisfactoria, se iluminará el icono en verde. A partir de este momento, el terminal móvil se encuentra adscrito a la red con

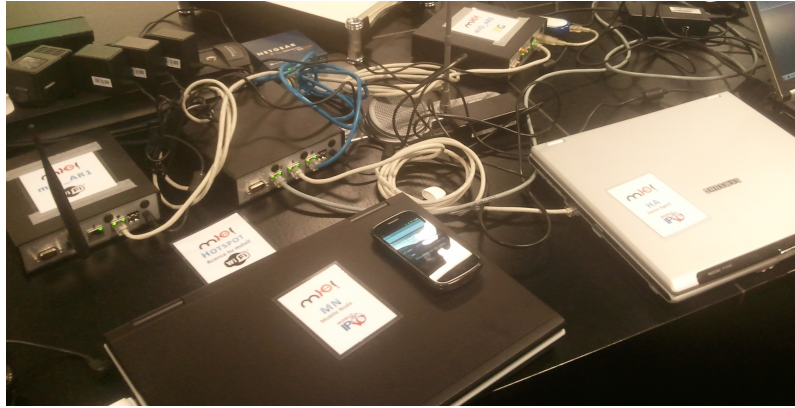


Figura 6.44: Imagen del entorno de pruebas

soporte móvil y el servidor estará accesible. La configuración de la red será la presentada en la figura 6.41.

Al iniciar la escucha o la visualización, el usuario comprobará como se incrementa el valor que refleja el tráfico de bajada. Para realizar el traspaso a la red IEEE 802.11 debe acercarse el móvil a la etiqueta NFC. Este procedimiento puede simular la entrada de un usuario a una cafetería que ofrezca conexión inalámbrica a sus clientes o la entrada en su casa.

La lectura de la etiqueta activa la interfaz IEEE 802.11. Dado que el sistema operativo Android no permite la conexión simultánea a dos o más redes, una vez se ha finalizado el proceso de conexión WiFi se desconecta de la red móvil. El éxito en el traspaso se puede observar en la parte central, donde el flujo de descarga se dirige ahora a través de la interfaz IEEE 802.11. La sesión de reproducción no se interrumpe, gracias al almacenamiento temporal y al entorno de movilidad MIPv6 que mantiene la conectividad extremo a extremo.

Para retornar el flujo a la interfaz de banda ancha, el usuario tendrá dos opciones, desactivar la interfaz IEEE 802.11 o salirse del radio de acción de la red a la que esté conectado.

6.4.4. Evaluación de rendimiento

El experimento realizado se puede evaluar desde dos puntos de vista: rendimiento con datos cuantitativos y operativa subjetiva o experiencia de usuario. Si bien los primeros repercuten notablemente en la experiencia de usuario no siempre es así, ya que se pueden encontrar mecanismos para diluir su influencia. La figura 6.44 incluye una imagen del escenario de pruebas configurado.

La evaluación del rendimiento se ha hecho principalmente empleando ordenadores portátiles por la flexibilidad de configuración que ofrecen y la disponibilidad de herramientas de medidas adecuadas. Se ha empleado la utilidad *Iperf* [240] para evaluar tres escenarios diferentes de traspaso: utilizando una única interfaz IEEE 802.11 en el MN, utilizando dos interfaces IEEE 802.11 y utilizando una interfaz IEEE 802.11 y otra GPRS/UMTS. Los dos primeros suponen un traspaso horizontal, mientras que el tercero es un traspaso vertical.

En todos los casos se han transmitido 10000 paquetes UDP de 1000 *bytes* desde el CN al MN, forzando el traspaso de forma manual hacia la mitad de la duración del experimento. En el traspaso vertical se ha restringido el ancho de banda con el que emite la fuente a 500 *Kbytes/seg*, pues de otra forma se satura el canal de comunicaciones GPRS/UMTS y se distorsiona la medida realizada, ya que las pérdidas de paquetes se incrementan por causas ajenas al propio traspaso. Por tanto, las pérdidas de paquetes que se detecten en los experimentos serán únicamente debidas a los procedimientos implicados en el traspaso. Cabe señalar que durante el proceso de medida se ha modificado la configuración explicada anteriormente para incluir un segundo punto de acceso inalámbrico IEEE 802.11.

La figura 6.45 presenta la evolución del traspaso para los tres escenarios en función del tiempo. La degradación de la comunicación se muestra como una variable booleana que indica el éxito o no de la transmisión entre los extremos. La tabla 6.6 muestra el porcentaje de paquetes perdidos y la duración del traspaso.

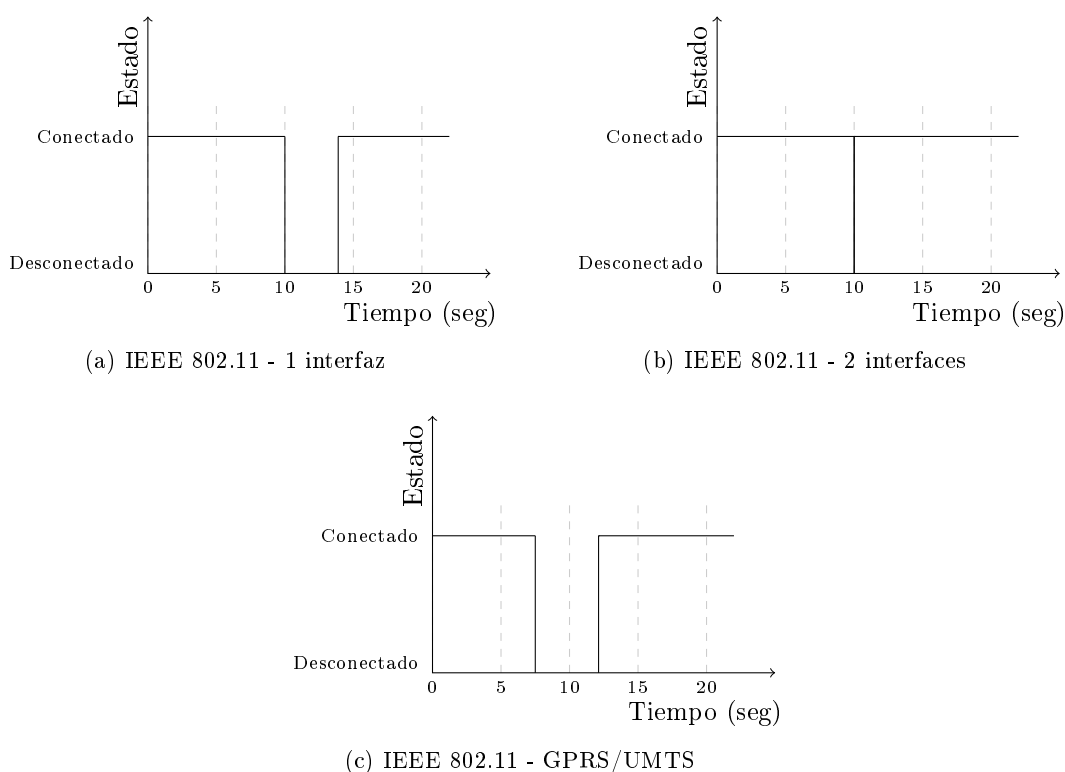


Figura 6.45: Evolución del traspaso

Para el primer caso, traspaso empleando una sola interfaz IEEE 802.11, se observa una pérdida de conexión entre los extremos algo inferior a los 4 segundos, coincidiendo aproximadamente con el tiempo de configuración de la conexión a la red inalámbrica. En esta configuración, el traspaso conlleva la desconexión de una red para conectarse a otra, puesto que la interfaz de red empleada no permite la conexión simultánea a dos redes. El tiempo de desconexión supone aproximadamente el 20 % del experimento, valor aproximado del porcentaje de paquetes perdidos. Como se ha insistido, el traspaso es guiado y no se rea-

Tabla 6.6: Rendimiento del traspaso MIPv6

Configuración	Pérdidas	Duración
IEEE 802.11 - 1 interfaz	19,00 %	3,890 seg
IEEE 802.11 - 2 interfaces	0,32 %	0,002 seg
IEEE 802.11 - GPRS/UMTS	26,00 %	4,620 seg

liza una búsqueda activa de la red de destino. En el caso de que se hubiera optado por esta opción las pérdidas hubiesen sido muy superiores, pues las interfaces inalámbricas no permiten paralelizar la transmisión/recepción y el escaneo activo.

A la vista del caso anterior, en el segundo escenario se pretende evaluar un traspaso ideal, en el que los tiempos de establecimiento de conexión a la red destino fueran nulos. Para ello se emplea un terminal con dos interfaces inalámbricas, cada una conectada a una red diferente. Se varía la configuración de `mip6d` para que soporte la comunicación por las dos interfaces, dando preferencia a una de ellas siempre que ésta esté activa. El haber fijado esta configuración no impide insistir en que, como se ha demostrado en el apartado 6.2, el uso de la UCL permite la gestión autónoma de las interfaces, lo que, ante una potencial detección de una situación de traspaso, habría activado la búsqueda de nuevas redes con la interfaz libre y configurado la conexión, redundando en un traspaso como el evaluado.

Se puede observar en la figura 6.45b que las pérdidas achacables al traspaso y la duración del mismo son prácticamente nulas. Ese pequeño porcentaje es debido a que internamente los procedimientos de MIPv6 sólo suponen actualizaciones de las tablas de rutas a las interfaces activas.

Las pruebas realizadas sobre este escenario han reportado un comportamiento cuanto menos reseñable, aunque no incide en la duración y volumen de pérdidas. La especificación MIPv6 no está diseñada para dar soporte a trasposos empleando dos interfaces radio, sino que está orientada a una única interfaz. Es por esto que en algunos casos se ha observado que, al retornar a la red origen manteniendo aún la conexión con la red en itinerancia, si bien el tráfico se envía por la interfaz preferente asociada a la red origen, los paquetes de retorno continúan recibándose por la otra interfaz. Esto es así pues, al no estar incluida esta circunstancia en la especificación, el nodo que actúa como HA mantiene la ruta que tenía activa para el retorno. Si se deshabilita esa interfaz en el MN, la ruta se modifica y tanto el paquete enviado como el recibido siguen el mismo camino.

Visto que al tener dos interfaces activas el traspaso se realiza de forma ideal, se plantea el tercer escenario, quizás más realista dado que es difícil que un terminal disponible en el mercado tenga dos interfaces IEEE 802.11. En esta ocasión, se emplea una interfaz IEEE 802.11 y otra GPRS/UMTS, replicando la configuración del teléfono móvil empleado para implementar el servicio y valorar la experiencia de usuario. Para este caso los resultados obtenidos se observan en la figura 6.45c. Hay que destacar que el tiempo de traspaso es de 4,6 segundos, en contra de lo esperado según el anterior experimento para dos interfaces WiFi. Por esta razón las pérdidas se elevan hasta un 26 % de los paquetes transmitidos. Se

considera que este comportamiento es debido a la gestión interna de los túneles IPv6 sobre IPv4 y la propia encapsulación de los paquetes sobre la red GPRS/UMTS. Adicionalmente, ese retraso puede ser causado porque durante el tiempo de inactividad se realice una liberación del canal GPRS/UMTS, lo que supondría que se deba restablecer nuevamente al activarse el traspaso. Este comportamiento requiere un estudio más profundo en el que no se ha incurrido durante este trabajo.

Es importante señalar que la evaluación del rendimiento realizada contrasta en cierta manera con el comportamiento obtenido de la evaluación del uso de un servicio multimedia a través del teléfono móvil. Durante los experimentos realizados, la experiencia de usuario fue satisfactoria, no observando cortes ni pérdidas de conexión que afectaran a la visualización o escucha. Esto es debido a que las pérdidas de paquetes pasan desapercibidas gracias al almacenamiento temporal que las aplicaciones de visualización de contenido multimedia incluyen. El volumen de información de respaldo disponible es suficiente como para cubrir la duración del traspaso. Durante algunas de las pruebas, la cantidad de datos temporales almacenada no fue suficiente y se observaron pequeñas interrupciones del servicio. No obstante, esa situación también se dio en algunas ocasiones visionando el vídeo sobre la red GPRS/UMTS, algo común y a lo que los usuarios están acostumbrados.

Adicionalmente, las impresiones mostradas por usuarios varios a los que se ha presentado la metodología de traspaso entre redes basada en NFC han sido positivas, corroborando los pensamientos iniciales a la hora de plantear esta operativa, es decir, sencillez y reducción del consumo de batería.

Capítulo 7

Conclusiones

La digitalización y el rápido avance tecnológico están abriendo oportunidades inimaginables hace unos años, que hacen que la sociedad se enfrente de una forma muy diferente a las situaciones más comunes de la vida cotidiana. Conscientes de que la tecnología puede ayudar a mejorar, la adopción global de ésta entre la ciudadanía ha sorprendido cualquier previsión. No es difícil encontrarse a alguien que lleva consigo múltiples dispositivos, como un ordenador portátil, un teléfono, una tableta, un reloj inteligente, un pulsómetro u otros sensores, entre otros.

Esta miríada de dispositivos está concebida para dar servicio al usuario, con objeto de proporcionar acceso a la información en cualquier instante y lugar de forma sencilla y amigable. Sin embargo, la situación más normal es la inversa y el usuario ha terminado por adaptarse a los propios dispositivos, haciendo frente a los tediosos y complejos procesos de configuración, superando el desconocimiento y las barreras que imponen.

Así, de los cinco atributos propuestos por Everett M. Rogers [241] que determinan «la adopción o el rechazo de una innovación incluyendo las tecnológicas: la ventaja relativa, la compatibilidad, la complejidad, la capacidad de ser probada, y la capacidad de ser observada», aún quedan varios por ser resueltos en el entorno presentado.

Por otro lado, la evolución de la relación entre los usuarios y sus dispositivos presenta un amplio recorrido de mejora hasta lograr la servidumbre completa por parte de estos últimos. En este sentido, a partir de una serie de casos de uso planteados como ejemplo de lo que el autor entiende que debería ser una PN, se han extraído una serie de requerimientos que toda PN tendría que cumplir y que han guiado el desarrollo de los trabajos.

Esta tesis ha presentado la PN como un novedoso modelo de red, que extiende los paradigmas de PAN e inteligencia ambiental (AI, *Ambient Intelligence*), y busca rellenar las carencias que las redes actuales presentan con respecto a la adaptación al usuario. De ahí surge la PN como una agrupación de todos los dispositivos de un usuario independientemente de sus características y de su localización y que habilita la comunicación heterogénea y segura entre ellos con el objetivo de hacer frente a las necesidades del usuario. Todos los nodos de una PN o nodos personales comparten una relación de confianza acreditada por el usuario.

El concepto de PN se centra en simplificar y favorecer la coexistencia de un usuario con

sus dispositivos y servicios. Esta búsqueda de sencillez ha llevado a reducir la complejidad y las restricciones de las arquitecturas de red tradicionales. Por esta razón, se concibe un nuevo modelo de arquitectura, basado en capas de abstracción. Se definen tres grandes niveles (frente a los siete del modelo OSI) vinculados con la conectividad a nivel de enlace, con la interacción a nivel de red y con la gestión de los servicios y se les dota de la libertad para intercambiar información entre ellos. Existe un cuarto nivel, asociado al contexto del usuario, sus dispositivos y la red que conforman, que, con una disposición transversal a los otros tres, habilita el flujo entre ellos.

Al abordar el estudio de los niveles de enlace y red, en esta tesis se ha detectado que la heterogeneidad en tipos de dispositivos es extensible a las tecnologías de comunicación disponibles en ellos. No se puede imaginar hoy en día un dispositivo con una única interfaz de comunicación. Para hacer frente a esa diversidad, se ha contribuido con la definición y posterior desarrollo de una UCL, que oculta al nivel de red toda la complejidad subyacente en cuanto a tecnologías de comunicaciones. Su diseño modular permite extender sus funcionalidades, entre las que se han presentado y evaluado la gestión autónoma de las interfaces de comunicaciones, el establecimiento de canales directos seguros entre nodos y la adquisición y utilización inteligente de estadísticas del canal de comunicaciones como parte del contexto. Los resultados experimentales obtenidos con la implementación realizada demuestran que la UCL va un paso más allá de las soluciones existentes en el ámbito de la optimización intercapas (*cross-layer optimization*), abriendo el camino hacia la aplicación de nuevas estrategias de comunicación cognitiva.

Solventados los problemas que la heterogeneidad plantea en las comunicaciones entre nodos a nivel de enlace, a nivel de red se ha definido primero cómo los nodos de usuario se agrupan y se comunican entre sí y, posteriormente, cómo nodos en diferentes agrupaciones establecen conexiones extremo a extremo.

Tratando mantener la independencia de los flujos de datos generados entre los nodos de las comunicaciones con nodos no personales, la arquitectura de red de la PN se ha basado en una red virtual superpuesta con un direccionamiento privado, cuya especificación se ha descrito en profundidad a lo largo de este trabajo. Todos los nodos de una PN por el mero hecho de pertenecer a un mismo usuario comparten una relación bilateral sobre la que se sustenta la confianza entre ellos y que es el elemento cohesionador de la red. Es por esto, que los *clusters*, según se han definido en la PN, no son sólo agregaciones de nodos próximos que pueden comunicarse entre sí, sino que se añade, como innovación, el requisito de que entre ellos exista esa relación de confianza mutua, métrica que además se ha usado para determinar las rutas más óptimas entre los nodos. La UCL, en colaboración con un módulo de descubrimiento de vecinos, permite identificar los nodos personales próximos y definir los límites del *cluster*. Dada la importancia del usuario en una PN, los nodos más próximos a él conforman un *cluster* especial que se ha denominado P-PAN.

Los *clusters* de una PN se generan de forma espontánea o predefinidos por el usuario y no tienen dependencia de la infraestructura. Por esta razón, se ha optado por emplear soluciones de encaminamiento ad-hoc para el enlace entre sus nodos. Por su parte, las comunicaciones entre nodos de diferentes *clusters* se apoyan en la infraestructura de interconexión, estableciendo túneles directos que encapsulan el tráfico personal. La solución de red presentada incluye también soporte para la movilidad, requerimiento indispensable a

cubrir si se trata de proporcionar una comunicación ubicua. Adaptando la solución especificada, ya desarrollada en el ámbito del proyecto MAGNET, en esta tesis se ha incluido la validación experimental de la movilidad empleando en una solución estándar como MIPv6 desplegado en dispositivos de usuario como teléfonos móviles inteligentes.

Si bien se ha descrito la posibilidad de emplear una arquitectura de red completamente distribuida, finalmente se ha optado por una solución híbrida con una entidad intermedia, el agente de la PN, que descarga de funcionalidades a los nodos de usuario durante el establecimiento de los canales de comunicación remotos y que, como se vio posteriormente, facilita además el mantenimiento de las relaciones de confianza dentro de la PN y la interacción entre PN.

Sobre la capa de red definida, los nodos intercambiarán la información asociada a los servicios. En esta tesis se ha propuesto una SMP que abarca todo el ciclo de vida de un servicio y que se ha dividido en cuatro grandes dominios funcionales: creación, publicación y descubrimiento, ejecución y provisión y plataforma de usuario. Se ha observado cómo las tareas que se realizan en cada uno de ellos se ven influenciados por el enfoque orientado al componente a la hora de definir un servicio y la heterogeneidad inherente a la PN.

En lo que a la arquitectura de la PN se refiere, por último, se dado respuesta a otro de los grandes requerimientos planteados al inicio de esta tesis, la adaptación al contexto. Esto se ha logrado a través de la capa transversal que unifica el tratamiento del contexto dentro de la PN. La SCMF, con una arquitectura funcional semejante a la SMP, proporciona las funcionalidades de descubrimiento, mantenimiento, procesado y distribución de la información de contexto. No todas ellas pueden ejecutarse dentro de cualquier nodo personal, razón por la que algunas de las tareas se delegan en los nodos con mayores capacidades. Como parte de las tareas de validación de la SCMF, se ha desarrollado y validado de forma simulada y en entorno real un procedimiento para el descubrimiento, elección y mantenimiento de aquel nodo que mejor puede acoger las funciones que requiere la SCMF.

Dentro de una PN se considera información de contexto no solo el entorno del usuario y sus dispositivos, sino también sus preferencias. La SCMF ofrece las interfaces que permiten al usuario o cualquier otro componente de la PN proporcionar información asociada al contexto, descrita según una ontología propia, y que será procesada internamente para dotarla de valor añadido. En este sentido, el desarrollo realizado para la validación de la UCL ha incorporado unas interfaces compatibles con las requeridas por la SCMF, a lo que se ha unido la adaptación de las estadísticas obtenidas a la ontología definida para la PN. La SCMF también incluye las interfaces de salida a través de las que obtener la información de contexto.

Hasta este punto se dieron repuesta a casi todos los requerimientos identificados (comunicaciones ubicuas, gestión de servicios, adaptación al contexto y facilidad de uso), restando únicamente los relacionados con la seguridad. Aunque en las descripciones de la arquitectura de la PN ya se fue haciendo mención a ciertos mecanismos de seguridad, para facilitar la comprensión se ha preferido aglutinar todos los aspectos de seguridad en un único punto.

Tomando como base los trabajos realizados en [107, 242, 243], se define la arquitectura de seguridad de la PN. Un nodo adquiere la condición de personal por pertenecer a un usuario. Sin embargo, para poder establecer una comunicación confiable con otro, debe ser capaz

de compartir su estatus. Dentro de esta tesis inicialmente se ha propuesto el empleo del PFP, mediante el cual y con la participación del usuario, dos nodos personales cualesquiera se reconocen entre sí y establecen una relación bilateral de confianza representada por una clave compartida. No obstante, la primera aproximación realizada mostró potenciales deficiencias al escalarla, lo que restaba atractivo a la PN. Por este motivo, se actualizó la definición, pasando de un enfoque completamente distribuido a uno que se sustenta en una PKI modificada y adaptada al entorno personal. El resultado del CPFPP es también el reconocimiento de la condición de personal entre dos nodos, pero mejora al PFP en que facilita la escalabilidad. En este sentido, esta tesis aporta una solución distribuida de gestión de CRL que trata de eliminar los riesgos de seguridad derivados del extravío de nodos personales. Adicionalmente, para dotar de mayor robustez a la capa de seguridad de la PN, se detalla una metodología jerárquica de diversificación de la clave bilateral según la capa de abstracción que se quiera asegurar. Este esquema se ha incluido en la implementación realizada de la UCL y es la base de la identificación de los nodos personales. Se ha demostrado de esta manera la viabilidad de la solución y lo sencillo que resulta para el usuario dotar de seguridad a las comunicaciones entre sus equipos.

Diseñada, especificada y validada la arquitectura de la PN, el siguiente paso ha sido definir la solución que permita a varias PN operar de manera colaborativa. Si los usuarios interaccionan entre sí, sus redes deben funcionar de la misma manera. De ahí surge el concepto de PN-F como el entorno en el que los usuarios comparten de forma ordenada y segura los recursos disponibles en su PN.

El establecimiento de una PN-F requiere de procedimientos más complejos que los planteados para la PN, puesto que debe garantizarse el cumplimiento de la voluntad de cada participante en la PN-F. En este sentido, se ha desarrollado el ciclo de vida completo de una PN-F. La descripción se inicia con la definición del perfil de la PN-F, en el que se detalla el objetivo y las condiciones a cumplir para participar en la PN-F, y del perfil de usuario o miembro, que enumera qué elementos y cómo, con quién y bajo qué circunstancias se comparten. Los perfiles guiarán el proceso de formación y uso de la PN-F. Ambos perfiles deberán tener condiciones comunes para que el potencial miembro pase a formar parte activa de la PN-F. Tras describir el funcionamiento de la PN-F, se define la especificación de una arquitectura genérica, que posteriormente se particulariza según dos enfoques. El primero considera la PN-F como la extensión natural de la PN y, por tanto, la define como una red virtual superpuesta. En este tipo de PN-F los usuarios pueden compartir cualquier recurso, ya sea capacidad de conexión o servicio. El otro planteamiento permite la formación de una PN-F considerando sólo los servicios. En ambos casos se ofrecen soluciones para dar soporte a PN-F originadas espontáneamente de forma ad-hoc o generadas a partir de un acuerdo preestablecido, dando respuesta a las necesidades observadas en los casos de uso.

Como no puede ser de otra forma, también se ha hecho especial énfasis en la seguridad y validación de las políticas de uso en los dos enfoques, para lo que se han dispuesto las entidades específicas que deben ser incorporadas a las PN. Además, ampliando la jerarquía de la PKI personal, se ha definido una nueva entidad que certifica la identidad y los perfiles de las PN. En este sentido, englobada en la validación experimental realizada, se ha propuesto una metodología basada en tarjetas inteligentes como elemento seguro para garantizar los procesos de puesta en marcha de una PNCA y facilitar el establecimiento de las relaciones seguras y confiables entre PN.

Aunque mencionado ya en las descripciones anteriores, hay que insistir en que los trabajos realizados no se han limitado a análisis teóricos, sino que las soluciones presentadas se han validado en entornos reales. Algunas de las más relevantes se han incluido en esta tesis, si bien en el ámbito de los proyectos de investigación en los que se ha participado durante los años en los que la investigación aquí reflejada se ha llevado a cabo (a destacar MAGNET, MAGNET Beyond o mIO! entre otros), se ha colaborado activamente en la integración y validación de la práctica totalidad de los componentes descritos.

Claramente en esta tesis se ha mostrado una solución para hacer frente a las redes personales y a la colaboración entre ellas. Aunque la mayoría de los protocolos y mecanismos que se han empleado están siendo ampliamente usados por la comunidad científica, aún se puede considerar que algunas de las propuestas están alejadas de la realidad tecnológica. No obstante, la adaptación de las soluciones planteadas a entornos más comunes y cercanos al usuario, sin abandonar la filosofía tras la PN y la PN-F, permitiría su aplicación más directa tal como se ha demostrado. En este sentido, y a modo ejemplo, los teléfonos de última generación ya soportan ciertos esquemas de gestión de la heterogeneidad en las comunicaciones y las comunicaciones multisalto se están aplicando con éxito para habilitar la conexión con y entre dispositivos sensores distribuidos en entornos de difícil acceso.

Los trabajos de estandarización que se están desarrollando en el ámbito de ECMA TC32 [244] y ETSI [245] se espera que den a conocer la PN y la PN-F a la industria y comiencen su paulatina integración. Con el nacimiento de la Internet de las Cosas (IoT, *Internet of Things*), se da por iniciada la transferencia de varias de las ideas consideradas en una PN. De una parte, los propios sensores se configuran, descubren e interaccionan de forma autónoma empleando protocolos de encaminamiento multisalto y manteniendo comunicaciones seguras tanto a nivel de enlace como extremo a extremo. De otra, la captura de datos del entorno realizada por los sensores permite inferir nuevos modelos de información con los que proporcionar servicios de valor añadido.

Tanto la PN como la PN-F han sido dos conceptos innovadores que se originaron unos años antes de la eclosión de las redes sociales como Facebook o Twitter. Las redes sociales, tal como se conocen actualmente, permiten a los usuarios compartir recursos multimedia personales, la localización o los pensamientos que se tengan en un momento dado. Sin embargo, no consideran la interacción entre los dispositivos que poseen. En este sentido, son reveladoras las palabras de uno de los creadores de Twitter, Evan Henshaw-Plath, quien durante el IV Congreso de Mentes Brillantes celebrado en Madrid postuló como conceptos futuristas que los dispositivos ofrezcan o generen información «en función de las circunstancias (dónde estemos, con quién estemos, nuestras constantes vitales, ...)» o el planteamiento de «una red que conecte a las personas que coinciden en una misma sala si necesidad de que ellos hagan nada», aspectos ambos ya considerados dentro de la PN y la PN-F.

7.1. Hacia la Internet del Futuro

Los conceptos de PN y PN-F se han planteado y analizado desde múltiples perspectivas a lo largo de esta tesis. No obstante, como arquitecturas abiertas que son, se ha dejado la posibilidad de introducir alternativas que permitan ir más allá de los resultados obtenidos

aquí. Como se ha comentado, el éxito de la PN y la PN-F vendrá dado por su aceptación y adopción por parte de la industria.

Se considera, por tanto, que la proyección natural de las tareas de investigación y desarrollo relacionadas con la PN y la PN-F es la extensión de los conceptos hacia la Internet del Futuro (FI, *Future Internet*). La FI consta de cuatro pilares apoyados sobre una nueva infraestructura de red como base. Esos pilares son la IoT, la Internet de los Servicios (IoS, *Internet of Services*), la Internet de los Contenidos y el Conocimiento (IoK, *Internet of Knowledge*) y la Internet de las Personas (IoU, *Internet of Users*), cuya correspondencia se observa en la figura 7.1. La coexistencia y convergencia de todos ellos proporcionará al usuario un entorno seguro, confiable y robusto a través del cual acceder de forma abierta, dinámica y descentralizada a la red y su información, al tiempo que se adaptará a las necesidades de los usuarios y su contexto. Desde su concepción, los trabajos en la PN y la PN-F han mantenido una línea dirigida, sin lugar a dudas, en esta dirección.

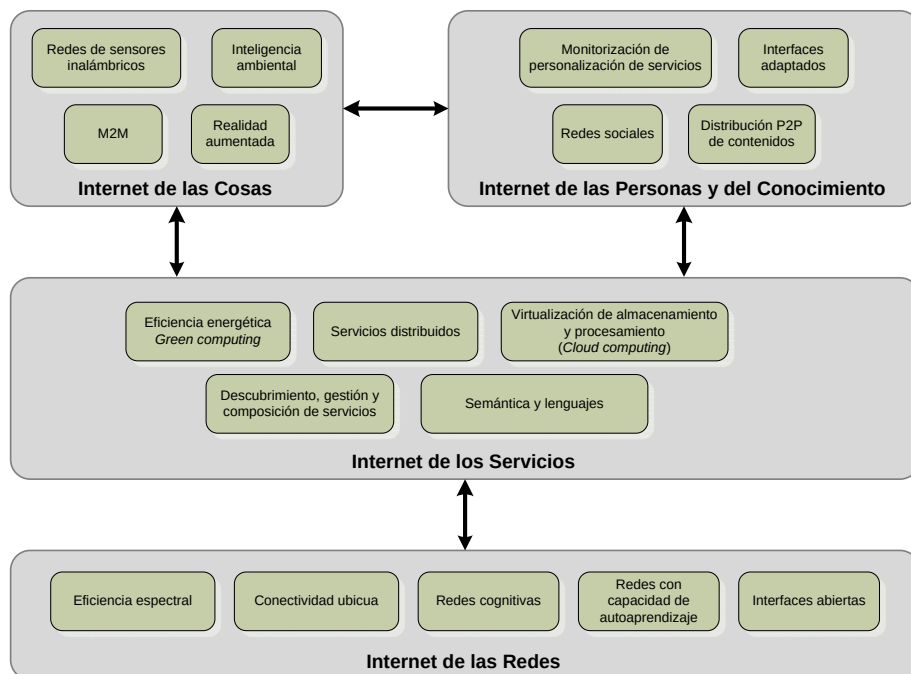


Figura 7.1: Arquitectura de la Internet del Futuro

Ya en las conclusiones se ha mostrado como los despliegues IoT incorporan ideas planteadas dentro de esta tesis, principalmente las encaminadas al establecimiento de la conectividad segura entre los nodos. En estos despliegues, cada nodo sensor captura información global de su entorno, la cual es analizada de forma conjunta con la de otros sensores para inferir información con un valor añadido. Los datos que se proporcionan suelen estar vinculados a un dominio más amplio que el delimitado a un solo sensor.

Por tanto, entre los retos a los que se enfrenta la IoT se incluye la investigación de nuevos métodos para transmitir datos de una manera dinámica, tanto síncrona como asíncrona, sobre entornos muy heterogéneos y su posterior procesamiento. Se deberá dimensionar de forma adecuada estas soluciones para mantener un equilibrio y no incurrir en errores pasados

que han llevado a saturar redes sin haber alcanzado las expectativas y desafíos tecnológicos planteados.

El modelo IoT ha desembocado, entre otros, en el paradigma de las ciudades inteligentes, explotado dentro del proyecto IST SmartSantander [246], donde se propone una plataforma de experimentación única en el mundo que dé soporte a los servicios de una ciudad inteligente. Su objetivo es diseñar, desplegar y validar una plataforma constituida por 20000 dispositivos (sensores, captadores, actuadores, cámaras, terminales móviles, etc.), que da origen a un espacio virtual donde los objetos se comunican entre sí y transmiten información útil con el fin de mejorar su calidad de vida de los ciudadanos.

De forma general, la información recogida por el conjunto de dispositivos IoT permite el desarrollo de numerosos servicios, que serán ofrecidos, utilizados o adaptados por un gran abanico de proveedores, consumidores o agregadores de servicio. Esta nueva manera de ofrecer funcionalidades fructifica en la IoS. Uno de los principales desafíos a los que se enfrenta la IoS comprende la integración de diferentes capas de servicios, desde servicios de infraestructura hasta servicios específicos con interfaz de usuario. La solución se encuentra en la orquestación inteligente de servicios y su personalización al contexto en el que se ejecuten, introducidas ambas en esta tesis, así como en el uso de la computación en la nube (*cloud computing*). Proyectos como CENIT mIO! han tratado de aplicar estas aproximaciones desde el punto de vista empresarial y de usuario. Los resultados obtenidos demuestran la viabilidad del planteamiento, pero también reportan que la tecnología requerida aún no está disponible al menos para el usuario final. Los numerosos obstáculos a superar dejan abierta la vía a explorar nuevos enfoques.

La implantación de los dos anteriores modelos tiene por el momento cierta independencia de la IoU. La IoU está muy vinculada a la IoK, en tanto en cuanto ambas tratan de aplicar la personalización al contexto y a las preferencias y necesidades de los usuarios como vía para proporcionar una mejor experiencia de uso, motivo por el cual se representan de forma conjunta en la figura 7.1. Para lograr este objetivo, se debe conocer más del usuario (sus costumbres, sus gustos, etc.) y de aquellos con los que se relaciona. El valor que tiene esa información se refleja directamente en las capitalizaciones de las compañías asociadas a las redes sociales, las cuales, aunque su modelo de negocio aún no está del todo claro, son las primeras en haber iniciado la captura de esos datos. No obstante, aunque se puedan adelantar los comportamientos de los usuarios y puesto que la tecnología es algo cada vez más cercano, los usuarios demandan también un mayor poder y autogestión.

Hay que mencionar que ya están surgiendo algunos proyectos planteando los pasos necesarios para hacer del usuario el centro del ecosistema. Es el caso del proyecto IST SOCIO-TAL [247] que persigue concebir técnicas que permitan la adopción de la IoT eliminando los temores que aspectos asociados privacidad y seguridad causan en el usuario.

Superar todas estas barreras descritas supone un gran reto para hacer realidad la FI. La PN y la PN-F han introducido un posible enfoque. Ahora es el momento de ofrecer nuevas alternativas por el beneficio de consumidores y proveedores.

Bibliografía

- [1] B. Gates, “Information At Your Fingertips, Keynote Speech”, en *COMDEX*, ép. MobiCom '04, Alladin Hotel, Las Vegas, Nevada, USA, nov. de 1994.
- [2] J. Kolari, ed., *Net in pocket?, Personal mobile access to web services*, ép. VTT publications 464. Espoo: VTT, 2002, 135, A 6, ISBN: 9513859835.
- [3] A. Whitten y J. D. Tygar, “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0”, en *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, ép. SSYM'99, Washington, D.C.: USENIX Association, 1999, págs. 14-14. URL: <http://dl.acm.org/citation.cfm?id=1251421.1251435>.
- [4] R. Kainda, I. Flechais y A. W. Roscoe, “Security and Usability: Analysis and Evaluation”, en *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, 2010, págs. 275-282.
- [5] P. Dourish, R. Grinter, J. Delgado de la Flor y M. Joseph, “Security in the wild: user strategies for managing security as an everyday, practical problem”, English, *Personal and Ubiquitous Computing*, vol. 8, n.º 6, págs. 391-401, 2004, ISSN: 1617-4909. URL: <http://dx.doi.org/10.1007/s00779-004-0308-5>.
- [6] E. A. R. Barbara Guttman, “An Introduction to Computer Security: The NIST Handbook”, English, Washington, inf. téc., 1995.
- [7] D. Balfanz, G. Durfee, D. Smetters y R. Grinter, “In search of usable security: five lessons from the field”, *Security Privacy, IEEE*, vol. 2, n.º 5, págs. 19-24, 2004, ISSN: 1540-7993.
- [8] L. Zhou y Z. Haas, “Securing ad hoc networks”, *Network, IEEE*, vol. 13, n.º 6, págs. 24-30, 1999, ISSN: 0890-8044.
- [9] Y.-C. Hu, A. Perrig y D. B. Johnson, “Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks”, *Wirel. Netw.*, vol. 11, n.º 1-2, págs. 21-38, ene. de 2005, ISSN: 1022-0038. URL: <http://dx.doi.org/10.1007/s11276-004-4744-y>.
- [10] J. Liu, F. Fu, J. Xiao e Y. Lu, “Secure Routing for Mobile Ad Hoc Networks”, en *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on*, vol. 3, 2007, págs. 314-318.

- [11] M. G. Zapata y N. Asokan, "Securing Ad Hoc Routing Protocols", en *Proceedings of the 1st ACM Workshop on Wireless Security*, ép. WiSE '02, Atlanta, GA, USA: ACM, 2002, págs. 1-10, ISBN: 1-58113-585-8. URL: <http://doi.acm.org/10.1145/570681.570682>.
- [12] P. Papadimitratos y Z. J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, n.º 2, págs. 343-356, feb. de 2006.
- [13] H. Yang, J. Shu, X. Meng y S. Lu, "SCAN: self-organized network-layer security in mobile ad hoc networks", *Selected Areas in Communications, IEEE Journal on*, vol. 24, n.º 2, págs. 261-273, 2006, ISSN: 0733-8716.
- [14] E. Gustafsson y A. Jonsson, "Always best connected", *Wireless Communications, IEEE*, vol. 10, n.º 1, págs. 49-55, 2003, ISSN: 1536-1284.
- [15] C. Perkins, *IP Mobility Support for IPv4, Revised*, RFC 5944 (Proposed Standard), Internet Engineering Task Force, nov. de 2010. URL: <http://www.ietf.org/rfc/rfc5944.txt>.
- [16] C. Perkins, D. Johnson y J. Arkko, *Mobility Support in IPv6*, RFC 6275 (Proposed Standard), Internet Engineering Task Force, jul. de 2011. URL: <http://www.ietf.org/rfc/rfc6275.txt>.
- [17] V. Devarapalli, R. Wakikawa, A. Petrescu y P. Thubert, *Network Mobility (NEMO) Basic Support Protocol*, RFC 3963 (Proposed Standard), Internet Engineering Task Force, ene. de 2005. URL: <http://www.ietf.org/rfc/rfc3963.txt>.
- [18] A. Gladisch, R. Daher y D. Tavangarian, "Survey on Mobility and Multihoming in Future Internet", English, *Wireless Personal Communications*, vol. 74, n.º 1, págs. 45-81, 2014, ISSN: 0929-6212. URL: <http://dx.doi.org/10.1007/s11277-012-0898-6>.
- [19] H. Naderi y B. E. Carpenter, "A Review of IPv6 Multihoming Solutions", en *Proceedings of the 10th International Conference on Networks*, St. Maarten, The Netherlands Antilles, ene. de 2011, págs. 145-149, ISBN: 978-1-61208-002-4.
- [20] M. Ghader, R. L. Olsen, L. Sanchez y col., "Resource and Service Discovery: PN Solutions", MAGNET (My personal Adaptive Global NET), Deliverable 2.2.1, dic. de 2004.
- [21] Telvent, ECSC, Robotiker y col., "Mecanismos para la orquestación de servicios", Proyecto CENIT mIO!, Entregable 4.7.1, ene. de 2011.
- [22] M. Baldauf, S. Dustdar y F. Rosenberg, "A Survey on Context-Aware Systems", *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 2, n.º 4, págs. 263-277, jun. de 2007, ISSN: 1743-8225. URL: <http://dx.doi.org/10.1504/IJAHUC.2007.014070>.
- [23] J. Hoebeke, G. Holderbeke, I. Moerman y col., "Personal network federations", en *Proceedings from the 15th IST Mobile and Wireless Communications Summit*, Mykonos, Greece, 2006.
- [24] MAGNET, *My personal Adaptive Global NET, FP6-IST-570102*, 2004. URL: <http://www.istmagnet.org> (Última visita en 2008).

-
- [25] MAGNET Beyond, *My personal Adaptive Global NET and Beyond*, FP6-IST-027396, 2006. URL: <http://www.ist-magnet.org> (Última visita en 2008).
- [26] mIO!, *Tecnologías para prestar servicios en movilidad en el futuro universo inteligente*, Proyecto CENIT, 2008. URL: <http://www.cenitmio.es> (Última visita en 2014).
- [27] PNP2008, *Personal Network Pilot 2008, Freeband Project*, 2004. URL: <http://pnp2008.freeband.nl> (Última visita en 2008).
- [28] E. Royer y C.-K. Toh, “A review of current routing protocols for ad hoc mobile wireless networks”, *Personal Communications, IEEE*, vol. 6, n.º 2, págs. 46-55, 1999, ISSN: 1070-9916.
- [29] M. Abolhasan, T. A. Wysocki y E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks”, *Ad Hoc Networks*, vol. 2, n.º 1, págs. 1-22, 2004.
- [30] C. Perkins, S. Ratliff y J. Dowdell, *Dynamic MANET On-demand (AODVv2) Routing*, draft-ietf-manet-aodvv2-03, Internet Engineering Task Force, feb. de 2014. URL: <http://tools.ietf.org/id/draft-ietf-manet-aodvv2-03.txt>.
- [31] T. Clausen y P. Jacquet, *Optimized Link State Routing Protocol (OLSR)*, RFC 3626 (Experimental), Internet Engineering Task Force, oct. de 2003. URL: <http://www.ietf.org/rfc/rfc3626.txt>.
- [32] T. Clausen, C. Dearlove, P. Jacquet y U. Herberg, *The Optimized Link State Routing Protocol Version 2*, RFC 7181 (Proposed Standard), Updated by RFCs 7183, 7187, 7188, Internet Engineering Task Force, abr. de 2014. URL: <http://www.ietf.org/rfc/rfc7181.txt>.
- [33] J. Moy, *OSPF Version 2*, RFC 2328 (INTERNET STANDARD), Updated by RFCs 5709, 6549, 6845, 6860, Internet Engineering Task Force, abr. de 1998. URL: <http://www.ietf.org/rfc/rfc2328.txt>.
- [34] B. Williams y T. Camp, “Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks”, en *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ép. MobiHoc '02, Lausanne, Switzerland: ACM, 2002, págs. 194-205, ISBN: 1-58113-501-7. URL: <http://doi.acm.org/10.1145/513800.513825>.
- [35] I. Stojmenovic y J. Wu, “Broadcasting and activity-scheduling in ad hoc networks”, en *Stojmenovic (Eds.), Ad Hoc Networking, IEEE*, IEEE Press, 2004, págs. 205-229.
- [36] H. Yang, H. Luo, F. Ye, S. Lu y L. Zhang, “Security in mobile ad hoc networks: challenges and solutions”, *Wireless Communications, IEEE*, vol. 11, n.º 1, págs. 38-47, 2004, ISSN: 1536-1284.
- [37] H. Deng, W. Li y D. Agrawal, “Routing security in wireless ad hoc networks”, *Communications Magazine, IEEE*, vol. 40, n.º 10, págs. 70-75, 2002, ISSN: 0163-6804.
- [38] Wireless World Research Forum, *WWRF Book of Visions - Visions of the Wireless World*, dic. de 2001. URL: <http://www.wireless-world-research.org>.
- [39] WWRF, *Wireless World Research Forum*. URL: <http://www.wwrf.ch> (Última visita en 2014).

- [40] AN, *Ambient Networks, FP6-IST-507134*, 2004. URL: <http://www.ambient-networks.org> (Última visita en 2008).
- [41] AN P2, *Ambient Networks Phase 2, FP6-IST-027662*, 2006. URL: http://cordis.europa.eu/projects/rcn/80709_en.html (Última visita en 2014).
- [42] PACWOMAN, *Power Aware Communications for Wireless OptiMised personal Area Networks, FP5-IST-34157*, 2002.
- [43] F. Louagie, L. Muñoz y S. Kyriazakos, "Paving the Way for the Fourth Generation: A New Family of Wireless Personal Area Networks", en *Proceedings from the 12th IST Mobile and Wireless Communications Summit*, jun. de 2003.
- [44] SHAMAN, *Secure Heterogeneous Access to Mobile Applications and Networks, FP5-IST-25350*, 2000. URL: <http://www.ist-shaman.org> (Última visita en 2008).
- [45] C. Gehrman, C. Gehrman, T. Kuhn, K. Nyberg y P. Windirsch, "Trust model, communication and configuration security for Personal Area", en *Proceedings from the 11th IST Mobile and Wireless Communications Summit*, Thessaloniki, Greece, jun. de 2002.
- [46] C. Gehrman, K. Nyberg y C. J. Mitchell, *The personal CA – PKI for a Personal Area Network*, Thessaloniki, Greece, jun. de 2002.
- [47] MOBILIFE, *Mobi Life, FP6-IST-511607*, 2004. URL: www.ist-mobilife.org (Última visita en 2014).
- [48] M. Klemettinen, *Enabling Technologies for Mobile Services: The MobiLife Book*. Wiley Publishing, 2007, ISBN: 0470512903, 9780470512906.
- [49] VCE, *Virtual Centre of Excellence In Mobile and Personal Communications*, 1996. URL: <http://www.mobilevce.com> (Última visita en 2014).
- [50] J. Dunlop, R. C. Atkinson, J. Irvine y D. Pearce, *A Personal Distributed Environment for Future Mobile Systems*, Aveiro, Portugal, jun. de 2002.
- [51] J. Dunlop, "The Concept of a Personal Distributed Environment for Wireless Service Delivery", English, *Wireless Personal Communications*, vol. 42, n.º 3, págs. 431-444, 2007, ISSN: 0929-6212. URL: <http://dx.doi.org/10.1007/s11277-006-9186-7>.
- [52] S. Schwiderski-Grosche, A. Tomlinson y D. B. Pearce, "Towards the Secure Initialisation of a Personal Distributed Environment", Department of Mathematics, Royal Holloway, University of London, Tech. Rep. RHUL-MA-2005-09, jul. de 2005. URL: <http://www.rhul.ac.uk/mathematics/techreports>.
- [53] MyNet, *Nokia and CSAIL Collaboration Project*, 2004. URL: <http://projects.csail.mit.edu/nrcc/mynet-ua.php> (Última visita en 2014).
- [54] Arvind y J. Hicks, "A Mobile Phone Ecosystem: MIT and Nokia's Joint Research venture", *IEEE Intelligent Systems*, vol. 21, n.º 5, págs. 78-79, 2006, ISSN: 1541-1672.
- [55] D. Kalofonos, Z. Antoniou, F. Reynolds y col., "MyNet: A Platform for Secure P2P Personal and Social Networking Services", en *Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on*, 2008, págs. 135-146.

-
- [56] B. Ford, J. Strauss, C. Lesniewski-laas y col., “User-Relative Names for Globally Connected Personal Devices”, en *Proceedings of the 5th International Workshop on Peer-to-Peer Systems (IPTPS06)*, 2006.
- [57] B. Ford, “Unmanaged Internet Protocol: Taming the Edge Network Management Crisis”, *SIGCOMM Comput. Commun. Rev.*, vol. 34, n.º 1, págs. 93-98, ene. de 2004, ISSN: 0146-4833. URL: <http://doi.acm.org/10.1145/972374.972391>.
- [58] PUCC, *Nokia and CSAIL Collaboration Project*, 2007. URL: <http://www.pucc.jp/> (Última visita en 2014).
- [59] N. Saito y K. Kitagawa, “Overview of Peer-to-Peer Universal Computing Consortium (PUCC): Background, Current Status and Future Plan”, en *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, ene. de 2007, págs. 783-787.
- [60] K. Braun, J. Grollmann, M. Horn y col., “Universal Personal Networking”, en *Universal Personal Communications, 1993. Personal Communications: Gateway to the 21st Century. Conference Record., 2nd International Conference on*, vol. 1, 1993, 108-112 vol.1.
- [61] LifeWorks, “Unified Domains and Unified User Experiences”, Siemens, White Paper, feb. de 2004. URL: <http://neutron.ing.ucv.ve/fernandezl/Multimedia/Webtorials/LifeWorks.pdf> (Última visita en 2014).
- [62] D. Husemann, C. Narayanaswami y M. Nidd, “Personal mobile hub”, en *Wearable Computers, 2004. ISWC 2004. Eighth International Symposium on*, vol. 1, 2004, págs. 85-91.
- [63] R. Kravets, C. Carter y L. Magalhães, “A Cooperative Approach to User Mobility”, *SIGCOMM Comput. Commun. Rev.*, vol. 31, n.º 5, págs. 57-69, oct. de 2001, ISSN: 0146-4833. URL: <http://doi.acm.org/10.1145/1037107.1037115>.
- [64] P. Debaty y D. Caswell, “Uniform Web presence architecture for people, places, and things”, *Personal Communications, IEEE*, vol. 8, n.º 4, págs. 46-51, 2001, ISSN: 1070-9916.
- [65] P. Maniatis, M. Roussopoulos, E. Swierk y col., “The Mobile People Architecture”, *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 3, n.º 3, págs. 36-42, jul. de 1999, ISSN: 1559-1662. URL: <http://doi.acm.org/10.1145/329124.329153>.
- [66] 3GPP, “Service requirements for Personal Network Management (PNM); Stage 1”, 3rd Generation Partnership Project (3GPP), TS 22.259, jun. de 2008. URL: <http://www.3gpp.org/ftp/Specs/html-info/22259.htm>.
- [67] I. Niemegeers y S. Heemstra de Groot, “From Personal Area Networks to Personal Networks: A User Oriented Approach”, English, *Wireless Personal Communications*, vol. 22, n.º 2, págs. 175-186, 2002, ISSN: 0929-6212. URL: <http://dx.doi.org/10.1023/A:1019912421877>.
- [68] I. Niemegeers y S. Heemstra de Groot, “Research Issues in Ad-Hoc Distributed Personal Networking”, English, *Wireless Personal Communications*, vol. 26, n.º 2-3, págs. 149-167, 2003, ISSN: 0929-6212. URL: <http://dx.doi.org/10.1023/A:1025522402484>.

- [69] M. Glesner, T. Hollstein y T. Murgan, "System design challenges in ubiquitous computing environments", en *Microelectronics, 2004. ICM 2004 Proceedings. The 16th International Conference on*, dic. de 2004, págs. 11-14.
- [70] K. Patten y K. Passerini, "From personal area networks to ubiquitous computing: preparing for a paradigm shift in the workplace", en *Wireless Telecommunications Symposium, 2005*, abr. de 2005, págs. 225-233.
- [71] M. Alutoin, K. Ahola, S. Lehtonen y col., "Self-organisation and mobility in Personal Networks", en *8th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, sep. de 2005, págs. 318-322, ISBN: 87-90834-82-8.
- [72] L. Muñoz, L. Sánchez, J. Lanza y col., "A proposal for self-organizing Personal Networks", en *WWRF meeting 15*, Paris, France, dic. de 2005.
- [73] *IEEE 802.15 Working Group for WPAN*. URL: <http://www.ieee802.org/15/>.
- [74] *Mobile Ad-hoc Networks (manet)*, since 1997. URL: <http://datatracker.ietf.org/wg/manet/charter/>.
- [75] Zero Configuration Networking (Zeroconf) working group, since 1999. URL: <http://www.zeroconf.org/>.
- [76] UPnP Forum. URL: <http://www.upnp.org> (Última visita en 2014).
- [77] M. Petrova, M. Jacobson, S. Oosthoek y col., "Conceptual Secure PN Architecture", MAGNET (My personal Adaptive Global NET), Deliverable 2.1.1, dic. de 2004.
- [78] S. Deering y R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460 (Draft Standard), Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946, 7045, 7112, Internet Engineering Task Force, dic. de 1998. URL: <http://www.ietf.org/rfc/rfc2460.txt>.
- [79] R. Braden, *Requirements for Internet Hosts - Communication Layers*, RFC 1122 (INTERNET STANDARD), Updated by RFCs 1349, 4379, 5884, 6093, 6298, 6633, 6864, Internet Engineering Task Force, oct. de 1989. URL: <http://www.ietf.org/rfc/rfc1122.txt>.
- [80] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)", *IEEE Std 802.15.3*, págs. 1-315, 2003.
- [81] "IEEE Standard for Local and Metropolitan Area Networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)", *IEEE Std 802.15.4 (Revision of IEEE Std 802.15.4-2006)*, págs. 1-314, 2011.
- [82] P. Balamuralidhar, N. Marthur, M. De Sanctis y col., "MAC/RRM Schemes for WPAN (Update D3.3.2a)", MAGNET (My personal Adaptive Global NET), Deliverable 3.3.2b, dic. de 2005.
- [83] Y. Xue, J. Gerrits, H. Choi, Nikhil y K. Schoo, "Specification for Prototyping from PHY and Layer 2", MAGNET (My personal Adaptive Global NET), Deliverable 3.3.4b, dic. de 2005.

-
- [84] B. Quijano, M. Lobeira, J. Ryckaert y col., “RF architectures for PAN nodes – Final version”, MAGNET (My personal Adaptive Global NET), Deliverable 5.1.2b, sep. de 2005.
- [85] D. Noguet, F. Platbrood, B. Van Poucke y col., “Selected air interface of PAN nodes for implementation”, MAGNET (My personal Adaptive Global NET), Deliverable 5.1.3, jun. de 2005.
- [86] T. Tong, M. Lobeira, X. Popon y col., “Prototype specifications”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 5.3.1, jul. de 2006.
- [87] M. Laugeois, D. Noguet, X. Popon y col., “HDR Prototype test report”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 5.4.1, jul. de 2006.
- [88] L. Biard, D. Noguet, N. Sortur y col., “Complete MAGNET system platform towards Pilot Services”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 6.4.1, oct. de 2007.
- [89] E. Kovacs, J. Lanza, L. Sanchez y col., “MAGNET System Specification”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 1.1.1, oct. de 2006.
- [90] J. Sachs, R. Agüero, K. Daoud y col., “Generic abstraction of access performance and resources for multi-radio access management”, en *Advances in Mobile and Wireless Communications*, ép. Lecture Notes Electrical Engineering, F. István, J. Bitó y P. Bakki, eds., vol. 16, Springer Berlin Heidelberg, 2008, págs. 239-259, ISBN: 978-3-540-79040-2. URL: http://dx.doi.org/10.1007/978-3-540-79041-9_13.
- [91] R. Agüero, J. Choque, L. Sánchez y col., “Empowering Cross-Layer Optimization: Dynamic Context Awareness in an Heterogeneous Wireless Environment”, en *Proceedings of the 6th International Symposium on Wireless Personal Multimedia Communications, WPMC*, Padova, Italia, sep. de 2004, págs. 120-124.
- [92] R. Sanz, R. Agüero, L. Sánchez, J. Choque y L. Muñoz, “Aportación a la mejora de prestaciones de los protocolos TCP/IP en entornos inalámbricos y multi-salto”, en *Actas de las IV Jornadas de Ingeniería Telemática, JITEL*, Las Palmas de Gran Canaria, sep. de 2003, págs. 393-400.
- [93] L. Muñoz, R. Agüero, J. Choque y col., “Empowering next-generation wireless personal communication networks”, *Communications Magazine, IEEE*, vol. 42, n.º 5, págs. 64-70, mayo de 2004, ISSN: 0163-6804.
- [94] H. Hu, W. Zhou, S. Zhang y J. Song, “A Novel Network Selection Algorithm in Next Generation Heterogeneous Network for Modern Service Industry”, en *Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE*, 2008, págs. 1263-1268.
- [95] B. Xing y N. Venkatasubramanian, “Multi-constraint dynamic access selection in always best connected networks”, en *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on*, 2005, págs. 56-64.
- [96] C. Gu, Y. Zhang, W. Ma, N. Liu e Y. Man, “Universal modeling and optimization for multi-radio access selection”, en *Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on*, 2009, págs. 1-4.

- [97] D. Griffith, "Autonomous Migration with Admission Control for Mobiles Affected by Access Network Failures", en *Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on*, 2009, págs. 1-5.
- [98] M. García, R. Agüero, L. Muñoz y J. Irastorza, "Smart Enhancement of TCP Performance Over Lossy WLAN Channels Through the Combined Use of Link Layer Techniques", English, *Wireless Personal Communications*, vol. 37, n.º 1-2, págs. 91-103, 2006, ISSN: 0929-6212. URL: <http://dx.doi.org/10.1007/s11277-006-0962-1>.
- [99] P. Mahonen, L. Munoz, D. Melpignano y col., "Wireless IP adaptation layer: an open performance enhancement protocol architecture", en *Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on*, vol. 2, sep. de 2002, 525-529 vol.2.
- [100] G. Koudouridis, R. Agüero, E. Alexandri y col., "Generic link layer functionality for multi-radio access networks", en *Proceedings of the 14th IST Mobile and Wireless Communications Summit*, Dresden, Alemania, jun. de 2005.
- [101] L. Sanchez, J. Lanza, L. Muñoz y col., "Definition of full PAN/PN Network Terminal Prototyping System", MAGNET (My personal Adaptive Global NET), Deliverable 2.5.2, dic. de 2005.
- [102] L. Sánchez, J. Lanza, M. Bauer, R. L. Olsen y M. Girod Genet, "A Generic Context Management Framework for Personal Networking Environments", en *The Third Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, San Jose (CA), USA, jul. de 2006, págs. 1-8, ISBN: 0-7803-9792-4.
- [103] I. D. Chakeres, E. M. Royer y C. E. Perkins, "Dynamic MANET On-demand Routing Protocol", Internet Engineering Task Force, IETF Internet Draft, oct. de 2005, Work in Progress.
- [104] T. Clausen, C. Dearlove y P. Jacquet, "The Optimized Link-State Routing Protocol version 2", Internet Engineering Task Force, IETF Internet Draft, jun. de 2006, Work in Progress.
- [105] J. Lanza, L. Sánchez y L. Muñoz, "Performance Evaluation of a Cross-layer based Wireless Interface Dynamic Selection on WPAN/WLAN Heterogeneous Environments: An Experimental Approach", en *6th International Workshop on Applications and Services in Wireless Networks*, Berlin, Germany, mayo de 2006, págs. 139-146, ISBN: 3-8167-7111-4.
- [106] L. Sánchez, J. Lanza y L. Muñoz, "Experimental Assessment of a Cross-Layer Solution for TCP/IP Traffic Optimization on Heterogeneous Personal Networking Environments", *Lecture Notes in Computer Science*, vol. 4217, págs. 284-296, sep. de 2006, ISSN: 0302-9743.
- [107] S. Mirzdeh, C. Politis, K. Nyberg y col., "Final version of the Network-Level Security Architecture Specification", MAGNET (My personal Adaptive Global NET), Deliverable 4.3.2, feb. de 2005.
- [108] K. Masmoudi y H. Afifi, "A Cross-layer Aware Imprinting Protocol for Personal Networks", en *Networking and Services, 2007. ICNS. Third International Conference on*, jun. de 2007, págs. 51-51.

-
- [109] J. Hoebeke, "Adaptive Ad Hoc Routing and Its Application to Virtual Private Ad Hoc Networks", PhD in Telecommunications, INTEC Broadband Communication Networks groep (IBCN), Vakgroep Informatietechnologie (INTEC), Faculteit Ingenieurswetenschappen, University of Ghent, 2007, ISBN: 978-90-8578-172-1.
- [110] S. Murthy y J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", *Mob. Netw. Appl.*, vol. 1, n.º 2, págs. 183-197, oct. de 1996, ISSN: 1383-469X. URL: <http://dx.doi.org/10.1007/BF01193336>.
- [111] L. Sánchez, J. Lanza, L. Muñoz y K. A. M. Alutoin, "Securing the Communication in Private Heterogeneous Mobile Ad hoc Networks", *Wireless Personal Communications*, vol. 52, n.º 2, págs. 393-409, 2010, ISSN: 0929-6212.
- [112] W. Louati y D. Zeglache, "Network based Virtual Personal Overlay Networks using Programmable Virtual Routers", *IEEE Communications Magazine, Special Issue "Self Organization in Networks Today"*, vol. 43, n.º 8, págs. 86-94, ago. de 2005.
- [113] W. M. Eddy, "At What Layer Does Mobility Belong?", *IEEE Communications Magazine*, vol. 42, n.º 10, págs. 155-159, oct. de 2004.
- [114] R. Hinden y B. Haberman, *Unique Local IPv6 Unicast Addresses*, RFC 4193 (Proposed Standard), Internet Engineering Task Force, oct. de 2005. URL: <http://www.ietf.org/rfc/rfc4193.txt>.
- [115] R. Hinden y S. Deering, *Internet Protocol Version 6 (IPv6) Addressing Architecture*, RFC 3513 (Proposed Standard), Obsoleted by RFC 4291, Internet Engineering Task Force, abr. de 2003. URL: <http://www.ietf.org/rfc/rfc3513.txt>.
- [116] J. Lipman, P. Boustead, J. Chicharo y J. Judge, "Optimised Flooding Algorithms for Ad Hoc Networks", en *In the 2nd Workshop on the Internet, Telecommunications and Signal Processing (WITSP'03)*, Coolangatta, Gold Coast, Australia, dic. de 2003.
- [117] M. J. Fischer, "The Consensus Problem in Unreliable Distributed Systems (A Brief Survey)", en *Foundations of Computation Theory*, ép. Lecture Notes in Computer Science, vol. 158, London, UK: Springer-Verlag, 1983, págs. 127-140, ISBN: 3-540-12689-9.
- [118] D. Cavin, Y. Sasson y A. Schiper, "Consensus with Unknown Participants or Fundamental Self-Organization", English, en *Ad-Hoc, Mobile, and Wireless Networks*, ép. Lecture Notes in Computer Science, I. Nikolaidis, M. Barbeau y E. Kranakis, eds., vol. 3158, Springer Berlin Heidelberg, 2004, págs. 135-148, ISBN: 978-3-540-22543-0. URL: http://dx.doi.org/10.1007/978-3-540-28634-9_11.
- [119] R. Koodli, *Mobile IPv6 Fast Handovers*, RFC 5268 (Proposed Standard), Obsoleted by RFC 5568, Internet Engineering Task Force, jun. de 2008. URL: <http://www.ietf.org/rfc/rfc5268.txt>.
- [120] L. Sanchez, "Contribution to the Cross-Layer Optimization of Intra-Cluster Communication Mechanisms in Personal Networks", Tesis doctoral, Grupo de Ingeniería Telemática, Departamento de Ingeniería de Comunicaciones, Universidad de Cantabria, feb. de 2008.
- [121] R. Dijkman y M. Dumas, "Service-oriented design: a multi-viewpoint approach", *International Journal of Cooperative Information Systems*, vol. 13, n.º 4, págs. 337-378, dic. de 2004. URL: <http://eprints.qut.edu.au/622/>.

- [122] Open Mobile Alliance, “Converged Personal Network Service Core Technical Specification”, versión 1.0.1, 2013.
- [123] J. Lanza, L. Sánchez y L. Muñoz, “Cluster Head Selection and Maintenance over Heterogeneous Mobile Wireless Personal Area Networks. an experimental approach”, en *9th International Symposium on Wireless Personal Multimedia Communications*, San Diego (CA), USA, sep. de 2006.
- [124] C. Shirky, *What is p2p... and what isn't?*, 2000. URL: <http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html> (Última visita en 2014).
- [125] Sun Microsystems and Project Kenai, *JXTA, The Language and Platform Independent Protocol for P2P Networking*, 2001. URL: <https://jxta.kenai.com/> (Última visita en 2014).
- [126] W. Adjie-Winoto, E. Schwartz, H. Balakrishnan y J. Lilley, “The design and implementation of an intentional naming system”, *SIGOPS Oper. Syst. Rev.*, vol. 34, n.º 2, págs. 22-, abr. de 2000, ISSN: 0163-5980.
- [127] B. N. Schilit y M. M. Theimer, “Disseminating active map information to mobile hosts”, *IEEE Network*, vol. 8, n.º 5, págs. 22-32, 1994.
- [128] P. J. Brown, “The stick-e document: a framework for creating context-aware applications”, en *Proceedings of Electronic Publishing'96, Palo Alto*, Palo Alto (CA), USA, ene. de 1996, págs. 259-272. URL: <http://www.cs.kent.ac.uk/pubs/1996/396>.
- [129] N. S. Ryan, J. Pascoe y D. R. Morse, “Enhanced reality fieldwork: the context-aware archaeological assistant”, en *Computer Applications in Archaeology 1997*, V. Gaffney, M. van Leusen y S. Exxon, eds., ép. British Archaeological Reports, Oxford: Tempus Reparatum, oct. de 1998. URL: <http://www.cs.kent.ac.uk/pubs/1998/616>.
- [130] A. K. Dey y G. D. Abowd, “Towards a Better Understanding of Context and Context-Awareness”, *CHI 2000 Workshop on the What, Who, Where, When, and How of Context-Awareness*, 2000. URL: <http://www.dsv.su.se/fuse/int8/docs/context.pdf>.
- [131] J. Gwizdka, “What’s in the context?”, en *Proceedings of Computer Human Interaction 2000*, Hague, Netherlands, 2000.
- [132] S. Long, R. Kooper, G. D. Abowd y C. G. Atkeson, “Rapid Prototyping of Mobile Context-Aware Applications: The Cyberguide Case Study”, en *Proceedings of the Second Annual International Conference on Mobile Computing and Networking, White Plains*, New York, USA: ACM Press, 1996, págs. 97-107.
- [133] P. Floréen, M. Przybilski, P. Nurmi y col., “Towards a Context Management Framework for MobiLife”, en *14th IST Mobile and Wireless Communications Summit*, Dresden, Germany, 2005.
- [134] M. Grossmann, M. Bauer, N. Honle y col., “Efficiently Managing Context Information for Large-Scale Scenarios”, en *PERCOM '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, Washington, DC, USA: IEEE Computer Society, 2005, págs. 331-340, ISBN: 0-7695-2299-8.

-
- [135] M. Jacobsson, M. Alutoin, M. Bauer y col., “Specification of PN networking and security components”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 2.3.1, dic. de 2006.
- [136] R. L. Olsen, “Enhancement of Wide-Area Service Discovery using Dynamic Context Information”, PhD in Telecommunications, Center for TeleInFrastruktur (CTIF), Institut for Elektroniske Systemer, Aalborg Universitet, ene. de 2008, ISBN: 87-90834-69-0.
- [137] M. Bauer, J. Lanza, L. Sanchez y col., “Final interface specification for context aware components”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Internal Report 2.1.1, sep. de 2006.
- [138] L. Sanchez, J. Lanza y col., “Preliminary interface specification for context aware and L2/L3 interfaces”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Milestone 2.1.1, abr. de 2006.
- [139] M. Jacobsson, I. Niemegeers, Y. Gu y col., “PN secure networking frameworks, solutions and performance”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 2.3.2, jun. de 2008.
- [140] T. Strang y C. Linnhoff-Popien, “A context modeling survey”, en *Workshop on Advanced Context Modelling, Reasoning and Management, UbiComp 2004 - The Sixth International Conference on Ubiquitous Computing*, Nottingham, England, 2004.
- [141] H. Sugano, S. Fujimoto, G. Klyne y col., *Presence Information Data Format (PIDF)*, RFC 3863 (Proposed Standard), Internet Engineering Task Force, ago. de 2004. URL: <http://www.ietf.org/rfc/rfc3863.txt>.
- [142] OWL Working Group, *OWL Web Ontology Language Overview*, World Wide Web Consortium, feb. de 2004. URL: <http://www.w3.org/TR/2004/REC-owl-features-20040210/> (Última visita en 2014).
- [143] OWL Working Group, *OWL Web Ontology Language Guide*, World Wide Web Consortium, feb. de 2004. URL: <http://www.w3.org/TR/2004/REC-owl-guide-20040210/> (Última visita en 2014).
- [144] Telefónica I+D y Universidad de Cantabria, “Sistema de autenticación y pagos basado en NFC en modo P2P”, Proyecto CENIT mIO!, Entregable - Activo Experimental 4.5.3_AE_3, jun. de 2009.
- [145] Telefónica I+D y Universidad de Cantabria, “Configurador de parámetros de red empleando tecnologías NFC y tarjeta inteligente”, Proyecto CENIT mIO!, Entregable - Activo Experimental 4.5.3_AE_5, ene. de 2011.
- [146] A. Cascón, “Application of Near Field Communication technologies to embedded systems”, Proyecto Fin de Carrera - Ingeniero de Telecomunicación, Grupo de Ingeniería Telemática, Departamento de Ingeniería de Comunicaciones, Universidad de Cantabria, jun. de 2010.
- [147] D. Hankerson, A. J. Menezes y S. Vanstone, *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003, ISBN: 038795273X.

- [148] H. Hwang, G. Jung, K. Sohn y S. Park, “A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP”, en *Information Science and Security, 2008. ICISS. International Conference on*, ene. de 2008, págs. 164-170.
- [149] K. Haataja y K. Hypponen, “Man-In-The-Middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures”, en *Communications, Control and Signal Processing, 2008. ISCCSP 2008. 3rd International Symposium on*, mar. de 2008, págs. 1096-1102.
- [150] S. Mirzadeh, K. Masmoudi, S. Fouladgar y col., “First solutions for implementation of Key Management and Crypto techniques”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 4.2.1, dic. de 2006.
- [151] “IEEE Standard Specifications for Public-Key Cryptography”, *IEEE Std 1363-2000*, págs. i-, 2000.
- [152] “IEEE Standard Specifications for Public-Key Cryptography- Amendment 1: Additional Techniques”, *IEEE Std 1363a-2004 (Amendment to IEEE Std 1363-2000)*, págs. 1-159, 2004.
- [153] L. Law, A. Menezes, M. Qu, J. Solinas y S. Vanstone, “An efficient protocol for authenticated key agreement”, *Designs, Codes and Cryptography*, vol. 28, n.º 2, págs. 119-134, 2003.
- [154] NSA. (2005). NSA suite B cryptography, National Security Agency.
- [155] H. Krawczyk, *HMQR: A High-Performance Secure Diffie-Hellman Protocol*, Cryptology ePrint Archive, Report 2005/176, 2005.
- [156] A. P. Sarr, P. Elbaz-Vincent y J.-C. Bajard, *A Secure and Efficient Authenticated Diffie Hellman Protocol*, Cryptology ePrint Archive, Report 2009/408, 2009.
- [157] SafeNet/Rainbow Technologies, *SafeNet/Rainbow Technologies Password Usage Survey*, jun. de 2003. URL: http://www.safenet-inc.com/solutions/password_survey.asp (Última visita en 2008).
- [158] ISO, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*, ISO/IEC 15946, 2008.
- [159] ANSI, *Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography*, X9.63, 2011.
- [160] D. Cooper, S. Santesson, S. Farrell y col., *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC 5280 (Proposed Standard), Updated by RFC 6818, Internet Engineering Task Force, mayo de 2008. URL: <http://www.ietf.org/rfc/rfc5280.txt>.
- [161] P. Yee, *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC 6818 (Proposed Standard), Internet Engineering Task Force, ene. de 2013. URL: <http://www.ietf.org/rfc/rfc6818.txt>.
- [162] A. Arnes, “Public Key Certificate Revocation Schemes”, PhD in Telematics, Department of Telematics, Norwegian University of Science y Technology, feb. de 2000.

-
- [163] C. Neuman, T. Yu, S. Hartman y K. Raeburn, *The Kerberos Network Authentication Service (V5)*, RFC 4120 (Proposed Standard), Updated by RFCs 4537, 5021, 5896, 6111, 6112, 6113, 6649, 6806, Internet Engineering Task Force, jul. de 2005. URL: <http://www.ietf.org/rfc/rfc4120.txt>.
 - [164] B. Aboba, D. Simon y P. Eronen, *Extensible Authentication Protocol (EAP) Key Management Framework*, RFC 5247 (Proposed Standard), Internet Engineering Task Force, ago. de 2008. URL: <http://www.ietf.org/rfc/rfc5247.txt>.
 - [165] S. Winter y J. Salowey, *Update to the Extensible Authentication Protocol (EAP) Applicability Statement for Application Bridging for Federated Access Beyond Web (ABFAB)*, RFC 7057 (Proposed Standard), Internet Engineering Task Force, dic. de 2013. URL: <http://www.ietf.org/rfc/rfc7057.txt>.
 - [166] J. Daemen y V. Rijmen, *Fips pub 197: advanced encryption standard (aes)*, nov. de 2001.
 - [167] S. Frankel y S. Krishnan, *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*, RFC 6071 (Informational), Internet Engineering Task Force, feb. de 2011. URL: <http://www.ietf.org/rfc/rfc6071.txt>.
 - [168] S. Kent y K. Seo, *Security Architecture for the Internet Protocol*, RFC 4301 (Proposed Standard), Updated by RFC 6040, Internet Engineering Task Force, dic. de 2005. URL: <http://www.ietf.org/rfc/rfc4301.txt>.
 - [169] C. Kaufman, P. Hoffman, Y. Nir y P. Eronen, *Internet Key Exchange Protocol Version 2 (IKEv2)*, RFC 5996 (Proposed Standard), Updated by RFCs 5998, 6989, Internet Engineering Task Force, sep. de 2010. URL: <http://www.ietf.org/rfc/rfc5996.txt>.
 - [170] T. Dierks y E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.2*, RFC 5246 (Proposed Standard), Updated by RFCs 5746, 5878, 6176, Internet Engineering Task Force, ago. de 2008. URL: <http://www.ietf.org/rfc/rfc5246.txt>.
 - [171] S. Turner y T. Polk, *Prohibiting Secure Sockets Layer (SSL) Version 2.0*, RFC 6176 (Proposed Standard), Internet Engineering Task Force, mar. de 2011. URL: <http://www.ietf.org/rfc/rfc6176.txt>.
 - [172] P. Eronen y H. Tschofenig, *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*, RFC 4279 (Proposed Standard), Internet Engineering Task Force, dic. de 2005. URL: <http://www.ietf.org/rfc/rfc4279.txt>.
 - [173] U. Blumenthal y P. Goel, *Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)*, RFC 4785 (Proposed Standard), Internet Engineering Task Force, ene. de 2007. URL: <http://www.ietf.org/rfc/rfc4785.txt>.
 - [174] R. Agüero, J. Choque y L. Muñoz, "Analysis of IP-based communications over a real multi-hop testbed based on the DSR protocol", en *Proceedings of the 8th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Aalborg, Denmark, sep. de 2005.

- [175] R. Agüero, L. Muñoz, J. Choque, L. Sánchez y J. Lanza, “Estudio experimental de los protocolos IP en redes inalámbricas multi-salto basadas en el protocolo DSR”, en *V Jornadas de Ingeniería Telemática*, Vigo, Spain, sep. de 2005, págs. 217-224, ISBN: 84-8408-346-2.
- [176] R. Chen y W. Yeager, “Poblano: A Distributed Trust Model for Peer-to-Peer Networks”, Sun Microsystems, inf. téc., 2000.
- [177] E. Hammer-Lahav, *The OAuth 1.0 Protocol*, RFC 5849 (Informational), Obsoleted by RFC 6749, Internet Engineering Task Force, abr. de 2010. URL: <http://www.ietf.org/rfc/rfc5849.txt>.
- [178] D. Hardt, *The OAuth 2.0 Authorization Framework*, RFC 6749 (Proposed Standard), Internet Engineering Task Force, oct. de 2012. URL: <http://www.ietf.org/rfc/rfc6749.txt>.
- [179] Facebook, feb. de 2004. URL: <http://www.facebook.com> (Última visita en 2014).
- [180] Tuenti, 2006. URL: <http://www.tuenti.com> (Última visita en 2014).
- [181] LinkedIn, *World's Largest Professional Network*, mayo de 2003. URL: <https://www.linkedin.com> (Última visita en 2014).
- [182] Twitter, mar. de 2006. URL: <http://www.twitter.com> (Última visita en 2014).
- [183] I. Niemegeers y S. Groot, “FEDNETS: Context-Aware Ad-Hoc Network Federations”, English, *Wireless Personal Communications*, vol. 33, n.º 3-4, págs. 305-318, 2005, ISSN: 0929-6212. URL: <http://dx.doi.org/10.1007/s11277-005-0574-1>.
- [184] J. Zidbeck, T. Ahola, K. Ahola y col., “MAGNET system secure networking components implementation”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 6.2.1, mayo de 2007.
- [185] L. Sanchez, J. Lanza, K. Ahola y col., “PN related platform towards Pilot Services”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 6.3.1, dic. de 2007.
- [186] J. Hoebeke, I. Moerman, R. De Spiegelaere y col., “Performance and Functionality Analysis of the PN Platform”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 6.3.2, dic. de 2007.
- [187] Shared Service Provider Working Group, “Registration Authority (RA) Requirements, Federal PKI Policy Authority”, United States Government, Tech. Rep. Ene. de 2007. URL: <http://idmanagement.gov/sites/default/files/documents/RArequirements.pdf> (Última visita en 2014).
- [188] J. Zeiss, L. Sanchez y S. Bessler, “Policy driven formation of federations between personal networks”, en *Mobile and Wireless Communications Summit, 2007. 16th IST*, jul. de 2007, págs. 1-5.
- [189] H. Olesen, J. B., A. Butkus y col., “User requirements for PN to drive the definition of a valid architecture”, MAGNET (My personal Adaptive Global NET), Deliverable 1.1.1b, dic. de 2004.

-
- [190] Canonical Ltd. y Ubuntu community, *Ubuntu*, oct. de 2004. URL: <https://www.ubuntu.com> (Última visita en 2014).
- [191] Hildon Foundation, *Maemo*, mayo de 2010. URL: <https://www.maemo.org> (Última visita en 2014).
- [192] Nokia, *Nokia 770 Internet Tablet*, nov. de 2005. URL: http://en.wikipedia.org/wiki/Nokia_N770 (Última visita en 2014).
- [193] Nokia, *Nokia 810 Internet Tablet*, nov. de 2005. URL: http://en.wikipedia.org/wiki/Nokia_N810 (Última visita en 2014).
- [194] J. Lanza, “Propuestas para la identificación y acceso seguro en redes personales, Contribution to Secure Identification and Access in Personal Networks”, Master en Tecnologías de la Información y Comunicaciones en Redes, Department of Communications Engineering, University of Cantabria, jul. de 2008.
- [195] W. Rankl y W. Effing, *Smart Card Handbook*, 3rd. New York, NY, USA: John Wiley & Sons, Inc., 1997, ISBN: 0471967203.
- [196] Z. Chen, *Java Card Technology for Smart Cards: Architecture and Programmer's Guide*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2000, ISBN: 0201703297.
- [197] “Digital cellular telecommunications system (Phase2+); Technical realization of the Short Message Service (SMS)”, Tech. Spec. 100 901 v7.4.0, dic. de 1999, GSM 03.40 version 7.4.0 Release 1998.
- [198] “Digital cellular telecommunications system (Phase2+); Security Mechanisms for the SIM application toolkit; Stage 2”, Tech. Spec. 101 181 v8.3.0, ago. de 2000, GSM 03.48 version 8.3.0 Release 1999.
- [199] P. FIPS, “46-3: data encryption standard (des)”, *National Institute of Standards and Technology*, vol. 25, n.º 10, 1999.
- [200] ISO, *Identification cards — Integrated circuit(s) cards with contacts — Part 4: Organization, security and commands for interchange*, ISO/IEC 7816-4, 2013.
- [201] J. Border, M. Kojo, J. Griner, G. Montenegro y Z. Shelby, *Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations*, RFC 3135 (Informational), Internet Engineering Task Force, jun. de 2001. URL: <http://www.ietf.org/rfc/rfc3135.txt>.
- [202] WINE, *Wireless Internet NETworks, FP5-IST-10028*, 1999. URL: http://cordis.europa.eu/projects/rcn/57121_en.html (Última visita en 2014).
- [203] F. T. Maxim Krasnyansky Maksim Yevmenkin, *Universal TUN/TAP device driver*, 2002. URL: <https://www.kernel.org/doc/Documentation/networking/tuntap.txt> (Última visita en 2014).
- [204] J. Salim, H. Khosravi, A. Kleen y A. Kuznetsov, *Linux Netlink as an IP Services Protocol*, RFC 3549 (Informational), Internet Engineering Task Force, jul. de 2003. URL: <http://www.ietf.org/rfc/rfc3549.txt>.
- [205] Linux Foundation, *Netlink*, 2009. URL: <https://www.kernel.org/doc/Documentation/networking/tuntap.txt> (Última visita en 2014).

- [206] L. Sanchez, J. Lanza y L. Muñoz, “Energy Efficiency of Dynamic Interface Selection Mechanisms in Wireless Ad-Hoc Networks”, English, en *Mobile Networks and Management*, ép. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, K. Pentikousis, R. Agüero, M. García-Arranz y S. Papavassiliou, eds., vol. 68, Springer Berlin Heidelberg, 2011, págs. 188-197, ISBN: 978-3-642-21443-1.
- [207] L. Sánchez, J. Lanza y L. Muñoz, “Eficiencia Energética de un Mecanismo de Selección Dinámica de Interfaces en Redes Ad-hoc Inalámbricas”, en *X Jornadas de Ingeniería Telemática*, Santander, Spain, sep. de 2011, págs. 245-250, ISBN: 978-84-694-5948-5.
- [208] L. Sánchez, J. Lanza y L. Muñoz, “Optimisation of dynamic interface selection mechanisms on multi-radio devices in ad hoc networks”, *Electronics Letters*, vol. 45, n.º 11, págs. 558-559, mayo de 2009, ISSN: 0013-5194.
- [209] J. del Prado Pavon y S. Choi, “Link adaptation strategy for IEEE 802.11 WLAN via received signal strength measurement”, en *Communications, 2003. ICC '03. IEEE International Conference on*, vol. 2, 2003, 1108-1113 vol.2.
- [210] K. Balachandran, S. Kadaba y S. Nanda, “Channel quality estimation and rate adaptation for cellular mobile radio”, *Selected Areas in Communications, IEEE Journal on*, vol. 17, n.º 7, págs. 1244-1256, 1999, ISSN: 0733-8716.
- [211] M. Kochhal, L. Schwiebert y S. Gupta, “Role-based hierarchical self organization for wireless ad hoc sensor networks”, en *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, ép. WSNA '03, San Diego, CA, USA: ACM, 2003, págs. 98-107, ISBN: 1-58113-764-8. URL: <http://doi.acm.org/10.1145/941350.941364>.
- [212] C. Lin y M. Gerla, “Adaptive clustering for mobile wireless networks”, *Selected Areas in Communications, IEEE Journal on*, vol. 15, n.º 7, págs. 1265-1275, 1997, ISSN: 0733-8716.
- [213] C.-R. Dow, S.-F. H. J.-H. Lin and e Y.-W. Wang, “An efficient distributed clustering scheme for ad-hoc wireless”, *IEICE Trans. Communications*, vol. E85-B(8), págs. 1561-1571, 2002.
- [214] H. Pennington, A. Carlsson, A. Larsson y col., *D-BUS Specification*, versión 0.23, ene. de 2014. URL: <http://dbus.freedesktop.org/doc/dbus-specification.html> (Última visita en 2014).
- [215] D. Zeuthen, *HAL Specification*, versión 0.5.10. URL: <http://www.freedesktop.org/wiki/Software/hal/> (Última visita en 2014).
- [216] K. Fall y K. Varadhan, eds., *The ns Manual (formerly ns Notes and Documentation)*, The VINT Project, 2011. URL: www.isi.edu/nsnam/ns/doc/ns_doc.pdf (Última visita en 2014).
- [217] J. Hoebeke, I. Moerman, M. Jacobsson y col., “Architecture and Protocols for Ad-hoc Self Configuration, Interworking, Routing and Mobility”, MAGNET (My personal Adaptive Global NET), Deliverable 2.4.1, dic. de 2004.

-
- [218] AT4 wireless, Inabensa, Universidad de Cantabria, Universidad Politécnica de Cartagena y Centro Tecnológico de Telecomunicaciones de Cataluña, “Soporte de trasposos de tecnologías de comunicación en redes 3G y WLAN. Aspectos de admisión y QoS”, Proyecto CENIT mIO!, Entregable 6.5.6, dic. de 2011.
- [219] PC Engines, *alix2d13 System Board Product File*. URL: <http://www.pcengines.ch/alix2d13.htm> (Última visita en 2014).
- [220] OpenWrt. URL: <https://openwrt.org> (Última visita en 2014).
- [221] Voyage Linux. URL: <http://linux.voyage.hk> (Última visita en 2014).
- [222] Google y Samsung, *Nexus S (Crespo)*, 2010. URL: <http://www.samsung.com/ca/consumer/mobile/mobile-phones/smartphones/GT-I9020FSMBMC> (Última visita en 2014).
- [223] D. Johnson, C. Perkins y J. Arkko, *Mobility Support in IPv6*, RFC 3775 (Proposed Standard), Obsoleted by RFC 6275, Internet Engineering Task Force, jun. de 2004. URL: <http://www.ietf.org/rfc/rfc3775.txt>.
- [224] USAGI (UniverSAl playGround for Ipv6) Project, *Linux IPv6 Development Project*, 2008. URL: <http://www.linux-ipv6.org> (Última visita en 2014).
- [225] J. Arkko, V. Devarapalli y F. Dupont, *Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents*, RFC 3776 (Proposed Standard), Updated by RFC 4877, Internet Engineering Task Force, jun. de 2004. URL: <http://www.ietf.org/rfc/rfc3776.txt>.
- [226] UMIP, *Mobile IPv6 and NEMO for Linux*, 2013. URL: <http://umip.org> (Última visita en 2014).
- [227] *Quagga Routing Suite*, 2010. URL: <http://www.nongnu.org/quagga/> (Última visita en 2014).
- [228] *HostAP - hostapd and wpa_supplicant*. URL: <http://hostap.epitest.fi> (Última visita en 2014).
- [229] *Router Advertisement Daemon (radvd)*. URL: <http://www.litech.org/radvd/> (Última visita en 2014).
- [230] *WvDial*. URL: <http://freecode.com/projects/wvdial> (Última visita en 2014).
- [231] ARM Limited, *ARM Architecture Reference Manual, ARmv7-A and ARmv7-R edition*, 2007. URL: <http://liris.cnrs.fr/~mmrissa/lib/exe/fetch.php?media=armv7-a-r-manual.pdf> (Última visita en 2014).
- [232] J. Lanza, *Mobile IPv6 user space daemons for Android*, sep. de 2011. URL: <http://devjlanza.wordpress.com/2011/09/12/mobile-ipv6-user-space-daemons-for-android/> (Última visita en 2014).
- [233] J. Lanza, *Mobile IPv6 user space daemons in Linux (Ubuntu)*, sep. de 2011. URL: <http://devjlanza.wordpress.com/2011/09/11/mobile-ipv6-user-space-daemons-in-linux-ubuntu/> (Última visita en 2014).
- [234] NFC Forum. URL: <http://www.nfc-forum.org> (Última visita en 2014).

- [235] NFC Forum, “NFC Data Exchange Format (NDEF)”, Tech. Spec. NDEF 1.0, jul. de 2006.
- [236] NFC Forum, “NFC Record Type Definition (RTD)”, Tech. Spec. RTD 1.0, jul. de 2006.
- [237] NFC Forum, “URI Record Type Definition”, Tech. Spec. RTD-URI 1.0, jul. de 2006.
- [238] NFC Forum, “Text Record Type Definition”, Tech. Spec. RTD-Text 1.0, jul. de 2006.
- [239] NFC Forum, “Smart Poster Record Type Definition”, Tech. Spec. SPR 1.1, jul. de 2006.
- [240] NLANR/DAST, *Iperf, The TCP/UDP Bandwidth Measurement Tool*, versión 2.0.3, 2008. URL: <http://iperf.sourceforge.net> (Última visita en 2014).
- [241] E. M. Rogers, *Diffusion of Innovations, 5th Edition*, 5th. Free Press, 16 de ago. de 2003, ISBN: 0743222091.
- [242] I. Gkanas, V. Kaldanis, A. Markopoulos y col., “State of the Art and Functional Specification of Network-Level Security Architecture”, MAGNET (My personal Adaptive Global NET), Deliverable 4.3.1, sep. de 2004.
- [243] J. Jaen Pallares, H. Affi, M. Argyropoulos y col., “Selections and Implementation of protocols and solutions in the view of PN-Platform”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 4.1.2, feb. de 2007.
- [244] ECMA International TC32, “Personal Networks - Overview and Standarization Needs”, ECMA International, inf. téc., dic. de 2010. URL: <http://www.ecma-international.org/memento/TC32-PNF-M.htm>.
- [245] “eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth”, Tech. Rep. 102 431 v1.1.1, feb. de 2009.
- [246] SmartSantander, *FP7-IST-257992*, 2010. URL: <http://www.smartsantander.eu> (Última visita en 2014).
- [247] SOCIOTAL, *Creating a socially aware citizen-centric Internet of Things, FP7-IST-609112*, 2013. URL: <http://sociotal.eu/> (Última visita en 2014).
- [248] D. S. J. De Couto, D. Aguayo, J. Bicket y R. Morris, “A High-throughput Path Metric for Multi-hop Wireless Routing”, en *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*, ép. MobiCom '03, San Diego, CA, USA: ACM, 2003, págs. 134-146, ISBN: 1-58113-753-2. URL: <http://doi.acm.org/10.1145/938985.939000>.
- [249] R. Draves, J. Padhye y B. Zill, “Routing in Multi-radio, Multi-hop Wireless Mesh Networks”, en *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking*, ép. MobiCom '04, Philadelphia, PA, USA: ACM, 2004, págs. 114-128, ISBN: 1-58113-868-7. URL: <http://doi.acm.org/10.1145/1023720.1023732>.
- [250] B. Awerbuch, D. Holmer y H. Rubens, “High Throughput Route Selection in Multi-rate Ad Hoc Wireless Networks”, English, en *Wireless On-Demand Network Systems*, ép. Lecture Notes in Computer Science, R. Battiti, M. Conti y R. Cigno, eds., vol. 2928, Springer Berlin Heidelberg, 2004, págs. 253-270, ISBN: 978-3-540-20790-0. URL: http://dx.doi.org/10.1007/978-3-540-24614-5_19.

- [251] R. Agüero, “Contribución a la mejora de las prestaciones en redes de acceso inalámbricas no convencionales”, Tesis doctoral, Grupo de Ingeniería Telemática, Departamento de Ingeniería de Comunicaciones, Universidad de Cantabria, nov. de 2007.
- [252] M. García, “Contribución a la caracterización experimental y mejora de las prestaciones de la arquitectura IP sobre infraestructura WLAN”, Tesis doctoral, Grupo de Ingeniería Telemática, Departamento de Ingeniería de Comunicaciones, Universidad de Cantabria, 2010.
- [253] Elmar Bartel, *New test TCP program*, 1998.
- [254] Wireshark Foundation, *Wireshark*. URL: <http://www.wireshark.org> (Última visita en 2014).

Apéndice A

Caracterización del canal inalámbrico IEEE 802.11

A continuación se describe el escenario de comunicaciones sobre el que se han llevado a cabo las campañas de medida para la validación de las diferentes soluciones que dan soporte a la PN incluidas en esta tesis. Se detalla el proceso de caracterización del canal radio inalámbrico IEEE802.11ab y la descripción de las herramientas empleadas.

La figura A.1 muestra el plano de la planta -4 de la antigua localización del Departamento de Ingeniería de Comunicaciones (DICOM) de la UC en la Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación (ETSIIT), lugar de realización de las campañas. Este emplazamiento representa el escenario típico de interiores en el que los nodos transmisor y receptor están separados una distancia de no más de 15 metros, con presencia aleatoria de obstáculos en el canal de propagación. Dependiendo de los lugares donde se emplacen los nodos no habrá línea de vista entre ellos.

Aunque se trata de un local de oficinas, su disposición se asemeja a la disposición habitual de cualquier hogar. Se considera, por tanto, que su utilización permite evaluar y extraer conclusiones del comportamiento de los canales de comunicaciones radio IEEE 802.11 que podrán extrapolarse a situaciones reales de los usuarios.

A.1. Análisis del escenario

Como primer paso en la caracterización del entorno de medidas se debe determinar la calidad del enlace dependiendo de la posición en la que se encuentren los nodos.

Métricas como *Expected Transmission Count Metric* (ETX) [248], *Weighted Cumulative Expected Transmission Time* (WCETT) [249] o *Medium Time Metric* (MTM) [250] se han propuesto y empleado como valores con los que estimar la calidad de un enlace radio. Sin embargo, las limitaciones para recolectar los parámetros necesarios para calcularlas, hacen que su uso en entornos reales sea complicado. Sin embargo, la SNR, otra métrica que se ha demostrado adecuada para describir la calidad de un enlace [209, 210] resulta más sencilla de adquirir, pues los *drivers* de las tarjetas inalámbricas facilitan este valor. Por esta razón, se seleccionado la SNR como métrica para representar la calidad del canal.

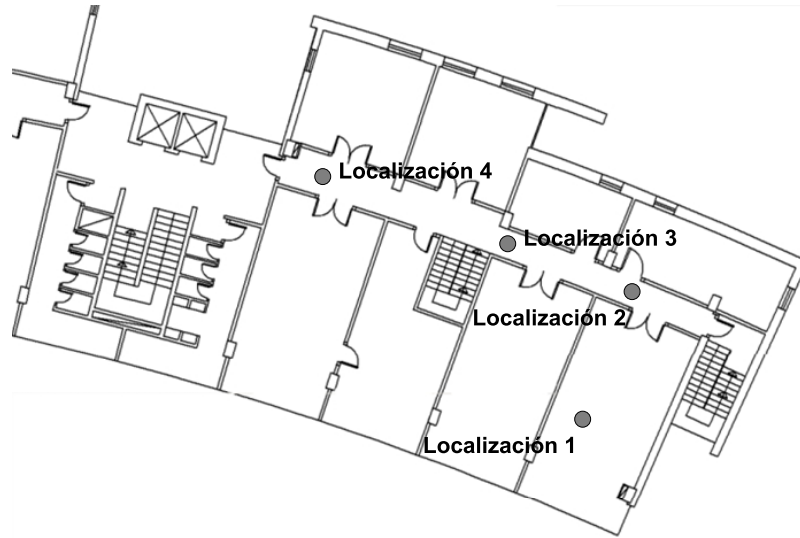


Figura A.1: Escenario de la campaña de medidas

Cada uno de los dos terminales empleados durante las medidas está equipado con dos interfaces inalámbricas, una IEEE 802.11a y otra IEEE 802.11b, emulando la heterogeneidad existente en los entornos de red personales. Además, el hecho de que estas tecnologías operen en diferentes zonas del espectro radioeléctrico, unido al hecho que emplean diferentes mecanismos sobre las capas física y MAC, permite que en cierta manera las conclusiones que se extraigan se puedan extrapolar a otras tecnologías inalámbricas que operen en un escenario similar.

La campaña de medidas se lleva a cabo realizando una transferencia de datos sobre UDP durante 30 segundos entre los nodos y analizando las estadísticas que se obtienen en el nodo receptor, nodo cuya posición varía según las condiciones de canal que se quieren estudiar. Todas las medidas se realizan empleado equipos donde el controlador de la tarjeta inalámbrica ha sido modificado para poder monitorizar las estadísticas a nivel de trama, como la SNR y la recepción correcta o errónea de las mismas.

Durante la realización de la batería de medidas, manteniendo uno de los terminales fijo, se han identificado cuatro localizaciones, tal como se muestra en la figura A.1, cuyas características se detallan a continuación. En la figura A.2 se muestra la distribución de la SNR detectada en las tramas recibidas en las diferentes localizaciones. Como se puede observar, cada una de las posiciones ofrece diferentes condiciones de canal, observándose una degradación progresiva según los nodos transmisor y receptor se separan. En este sentido, señalar que en la posición 4 únicamente se presentan los resultados para el canal IEEE 802.11b, pues las condiciones para el caso IEEE 802.11a resultaron ser muy malas y las medidas obtenidas no permiten describir de manera adecuada esa posición.

A la vista de esta representación, se puede concluir que la SNR se distribuye según una variable aleatoria gaussiana. Para visualizar esta apreciación se incluye la figura A.3, donde se comprueba cómo la campana se desplaza al variar la localización. La tabla A.1 muestran la media y desviación típica para cada una de las localizaciones. En [251, 252] se analiza

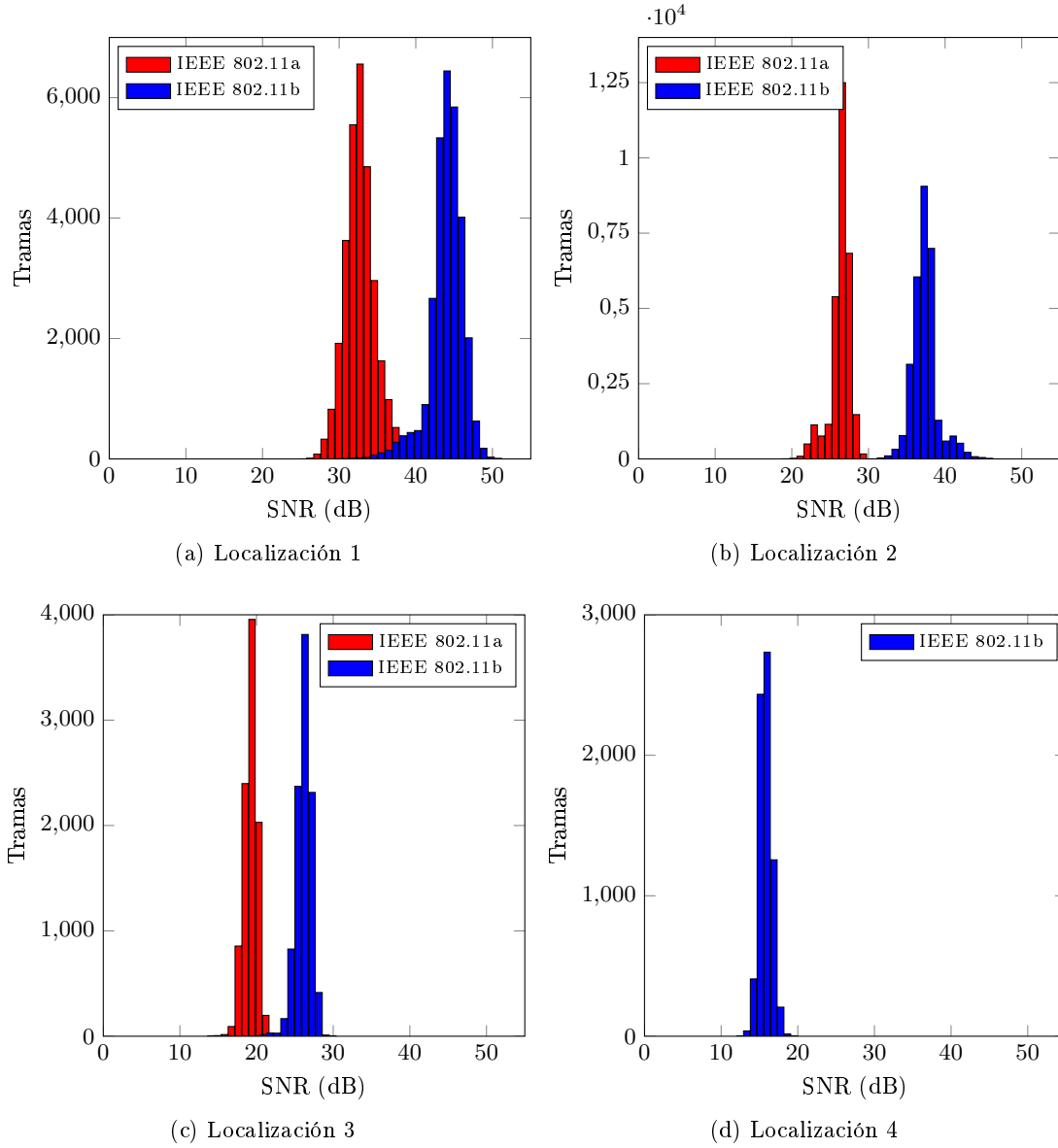


Figura A.2: Caracterización del canal en función de la SNR

en mayor profundidad este comportamiento a partir del cual se ha generado un modelo del canal inalámbrico tomando como base el comportamiento en un entorno real.

A.2. Rendimiento de las interfaces radio

Determinadas las zonas en las que se pueden fijar las condiciones del canal de comunicaciones como ideales, buenas, medias y malas, a continuación se procede a estudiar el rendimiento de los protocolos de transporte más comúnmente empleados, UDP y TCP, en

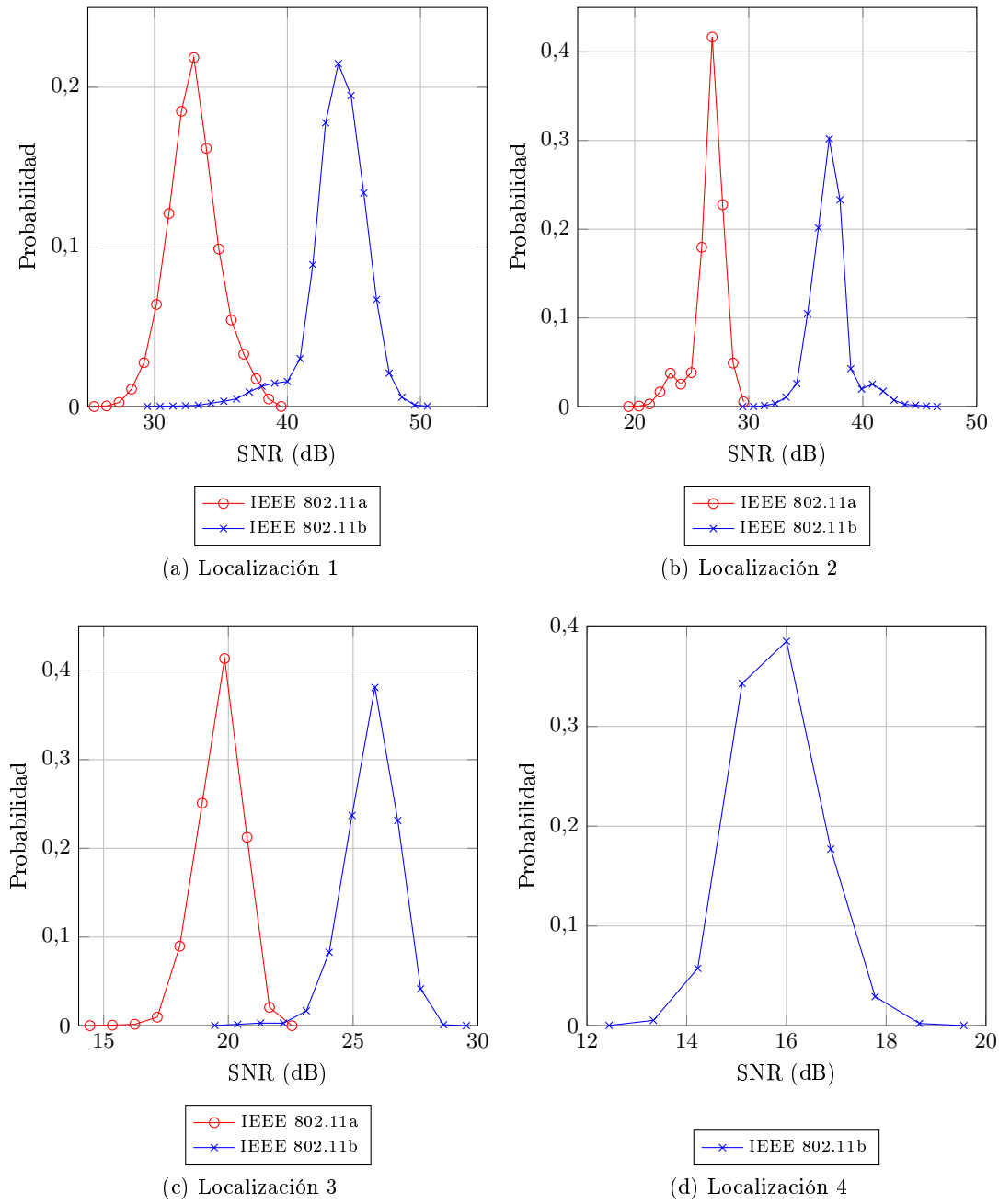


Figura A.3: Función de distribución de probabilidad de la SNR

cada una de las situaciones para cada una de las interfaces radio con las que se ha dotado a los terminales de prueba.

A.2.1. Tráfico UDP

En la tabla A.1 se muestran los resultados medios y la desviación estándar de los experimentos realizados para analizar el comportamiento con tráfico UDP. El procedimiento seguido durante la campaña de medidas consistió nuevamente en el envío de 10000 paquetes UDP de 1500 *bytes* entre dos nodos, desplazando uno de ellos entre ubicaciones que ofrecen diferentes SNR. La figura A.4 muestra la evolución del rendimiento en las cuatro posiciones.

Tabla A.1: Estadísticas de rendimiento de las interfaces IEEE 802.11 en UDP según la localización

Configuración	Rendimiento (Mbps)	FER (%)	SNR (dB)
<i>Localización 1</i>			
IEEE 802.11a	33,73±0,56	5,41 %±1,50	32,80±1,31
IEEE 802.11b	6,00±0,01	0,00 %±0,00	44,74±0,66
<i>Localización 4</i>			
IEEE 802.11a	26,98±3,77	23,58 %±10,09	26,00±1,42
IEEE 802.11b	5,87±0,10	0,03 %±0,03	35,92±1,45
<i>Localización 3</i>			
IEEE 802.11a	5,37±1,47	81,32 %±2,72	19,08±0,51
IEEE 802.11b	5,76±0,27	0,98 %±1,14	25,41±1,19
<i>Localización 4</i>			
IEEE 802.11b	3,01±0,38	22,94 %±6,23	16,56±1,01

En la localización 1 se observan unas condiciones de canal prácticamente ideales con una tasa de error de trama (FER, *Frame Error Rate*) casi despreciable, lo que supone que el número de paquetes perdidos es muy bajo. La figura A.4a muestra cómo durante casi todo el experimento el rendimiento se mantiene constante.

Al desplazar uno de los nodos a la ubicación 2 se detecta una degradación del rendimiento, especialmente notable para el canal IEEE 802.11a. Esto se refleja en la figura A.4b donde la variabilidad del ancho de banda instantáneo en torno a la media es elevada con desvanecimientos que llegan incluso a niveles cercanos a los de IEEE 802.11b. Para IEEE 802.11b, por el contrario, la reducción de SNR prácticamente no afecta al rendimiento manteniéndose la FER en mínimos. No obstante, considerando tanto el rendimiento como la FER, la interfaz más adecuada en esta localización sigue siendo IEEE 802.11a.

En la localización 3 el volumen de paquetes perdidos en las transmisiones realizadas para IEEE 802.11a llega a cotas que supondrían una degradación inaceptable de cualquier aplicación que usara este canal. Sin embargo, el rendimiento de IEEE 802.11b se mantiene estable si bien se aprecia un pequeño incremento de la FER, pero aún en límites aceptables.

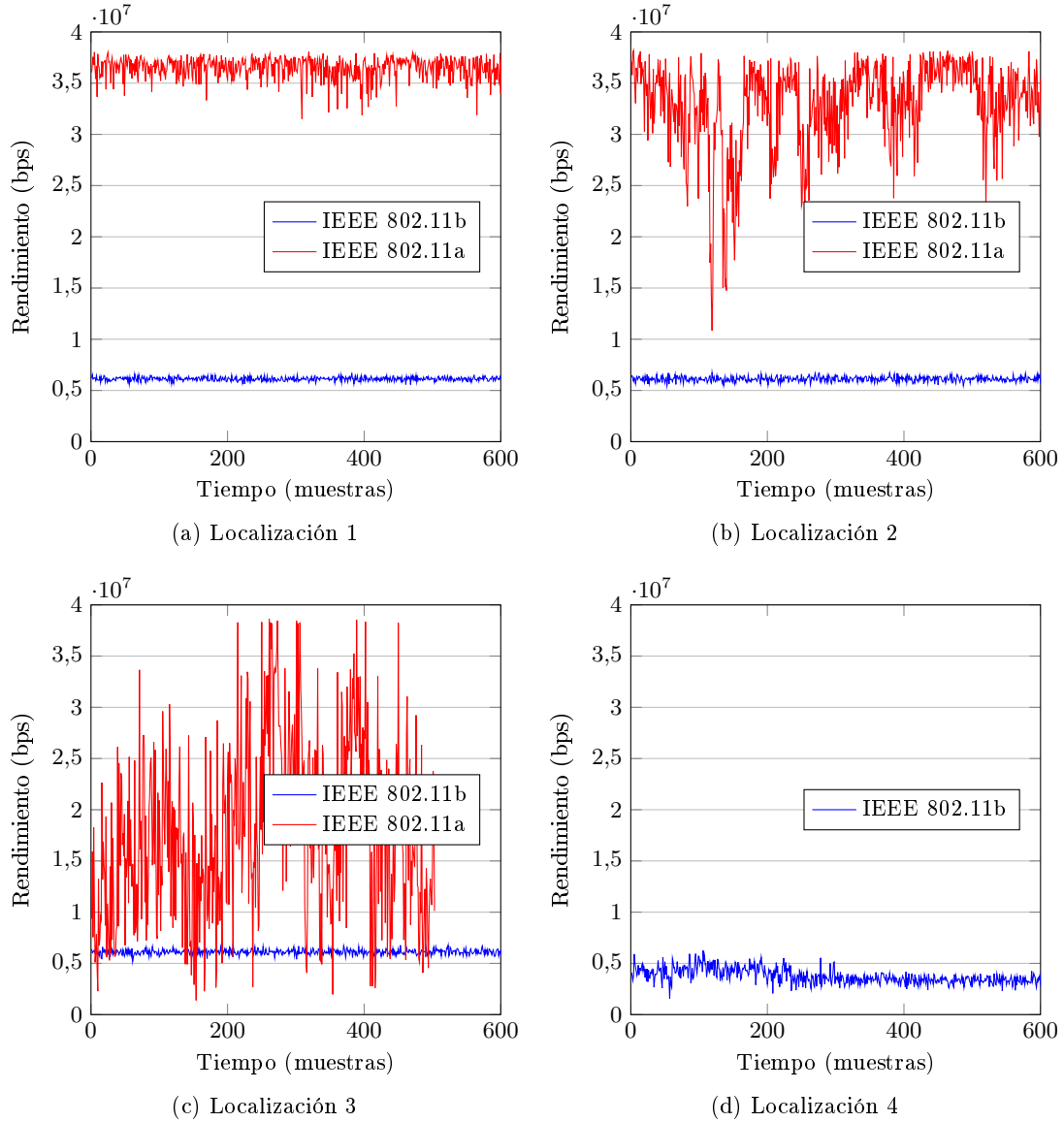


Figura A.4: Evolución del rendimiento de las interfaces IEEE 802.11 en UDP según la localización

Observando el rendimiento instantáneo en la figura A.4c, aunque en media IEEE 802.11a ofrece un rendimiento algo mejor que IEEE 802.11b, la mejora no es excesiva y los niveles de pérdidas hacen que se considere más adecuado el uso de IEEE 802.11b en esta situación.

Por último, en la localización 4 el rendimiento es pobre tanto para IEEE 802.11a como IEEE 802.11b, como se observa en la figura A.4d. Es más, para el caso de IEEE 802.11a las pérdidas de paquetes son tan elevadas que es imposible establecer una comunicación entre los nodos y extraer conclusiones de su transmisión. Por su parte, aunque con una tasa FER

más alta y una menor estabilidad del rendimiento del canal, la calidad del enlace IEEE 802.11b se puede considerar todavía aceptable.

Finalizado el estudio del canal inalámbrico usando tráfico UDP, se considera que a partir de niveles de SNR por debajo de 25 dB es más recomendable el uso de IEEE 802.11b dada la gran degradación del canal.

A.2.2. Tráfico TCP

Debido a que TCP se diseñó para su uso en redes cableadas, donde las pérdidas se consideran debidas a colisiones por congestión del canal, los mecanismos de control de congestión que fuerzan al transmisor a parar cuando se detectan estas situaciones funcionan bien en estas redes, pero en las inalámbricas, donde las pérdidas se deben a la deficiencia en el canal, estas soluciones no son válidas.

Para analizar el comportamiento de TCP se realizó la transmisión de un fichero de 10 *Mbytes* empleando FTP. En la tabla A.2 se resumen los resultados obtenidos de la batería de pruebas. Las métricas empleadas incluyen el número de paquetes fuera de orden, el número máximo de retransmisiones de un mismo paquete y el tiempo medio entre ellas, así como el tiempo que el transmisor se queda en espera debido a la activación de los mecanismos de control de congestión.

Tabla A.2: Estadísticas de rendimiento de los interfaces IEEE 802.11 en TCP según la localización

Configuración	Rendimiento (Mbps)	Paquetes totales	Paquetes fuera de orden	Tpo. inactivo (ms)	Rtx. (total)
<i>Localización 1</i>					
IEEE 802.11a	28,08±0,27	7320±9	74±8	20,96±15,56	75±9
IEEE 802.11b	5,10±0,01	7289±18	7±2	107,02±3,15	7±2
<i>Localización 2</i>					
IEEE 802.11a	9,48±3,44	7550±84	280±82	1577,28±2427,82	305±84
IEEE 802.11b	5,08±0,07	7286±21	6±2	109,94±4,52	6±2
<i>Localización 3</i>					
IEEE 802.11a	2,42±1,16	7758±226	397±156	3483,98±2960,45	513±226
IEEE 802.11b	5,12±0,03	7278±22	17±6	98,90±8,51	17±6
<i>Localización 4</i>					
IEEE 802.11b	3,11±1,11	7587±201	289±161	544,85±169,07	342±201

Como sucedió para el caso de UDP, en la localización 1 el canal de comunicaciones se puede considerar ideal y el número de retransmisiones y errores es mínimo. En estas

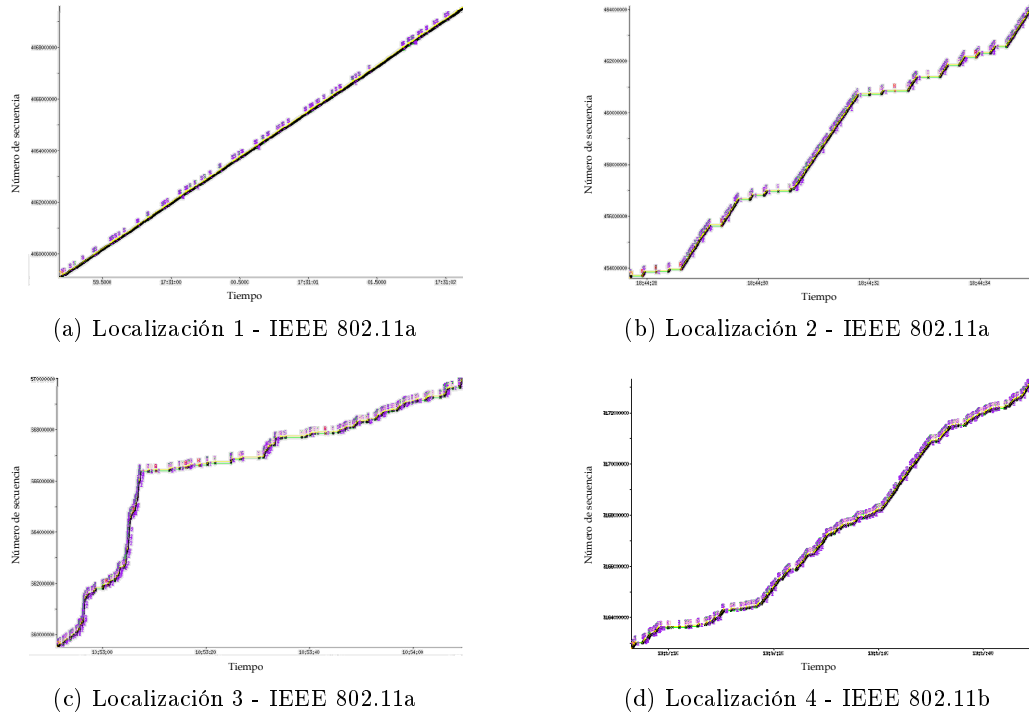


Figura A.5: Evolución del rendimiento de las interfaces IEEE 802.11 en TCP según la localización

condiciones la interfaz más adecuada es IEEE 802.11a con unas tasas de transferencia de aproximadamente 28 Mbps (pendiente de la gráfica de la figura A.5a).

En la localización 2, el número de retransmisiones para el canal IEEE 802.11a se ve incrementado, pero su patrón de ocurrencia no hace que se disparen los mecanismos de control de congestión. No obstante, en alguno de los experimentos realizados las ráfagas de error provocan tiempos de inactividad elevados, lo que redundará en un bajo rendimiento. En esta situación, el comportamiento todavía no es muy errático e IEEE 802.11a se puede considerar todavía la opción más óptima.

En la localización 3, el comportamiento observado anteriormente se ve agravado, lo que hace que el rendimiento de IEEE 802.11b sea ya mejor que el de IEEE 802.11a debido a los continuos períodos de inactividad en los que incurre el transmisor en el segundo caso.

Las condiciones del canal IEEE 802.11a en la localización 4 están tan degradadas que impiden la adquisición de estadísticas. Este comportamiento contrasta con el del IEEE 802.11b que aún muestra un rendimiento aceptable, aunque con un elevado número de retransmisiones. La figura A.5d presenta como la evolución de la transmisión ya no es tan lineal como en el resto de las localizaciones, aunque no se observan períodos de inactividad.

La evaluación realizada demuestra que el rango de SNR para el que se puede considerar TCP vulnerable a las deficiencias del canal es más amplio que para UDP. No obstante, el

límite de 25 dB obtenido para UDP como SNR a partir de la cual es más recomendable el uso de IEEE 802.11b frente a IEEE se puede considerar también válido para TCP.

A.3. Herramientas de medida empleadas

Las herramientas usadas en el proceso de medida se enumeran a continuación:

- **nttcp** [253]: generador de tráfico *software* basado en un modelo cliente-servidor. Permite el empleo de conexiones tanto UDP como TCP. Su uso se ha extendido mucho entre usuarios de Linux y redes de computadores, ya que se trata de una poderosa herramienta de análisis para medir el rendimiento que se puede alcanzar en una determinada red, pues una vez que termina una conexión devuelve la tasa binaria alcanzada durante la misma y las pérdidas de paquetes en las que se ha incurrido.
- **iperf** [240]: programa similar a nttcp y que, al igual que éste genera tráfico basado en un modelo cliente-servidor, de nuevo, soportando conexiones tanto UDP como TCP. En la mayoría de las medidas realizadas se ha utilizado esta herramienta, por permitir más parámetros de configuración que nttcp. Así, por ejemplo, permite modificar la ventana TCP, la MTU o el flujo de datos transmitidos en el caso de UDP. Como salida, ofrece información del *throughput* obtenido a lo largo de la transmisión y un valor final del rendimiento medio alcanzado durante la misma.
- **Wireshark** [254]: analizador de protocolos gratuito que permite examinar datos de una captura realizada durante una transmisión. Dispone de numerosos disectores que permiten el análisis avanzado de protocolos como Ethernet, IP, TCP y UDP, entre otros.

Apéndice B

Publicaciones

En este anexo de la tesis se resumen todas las publicaciones que de alguna manera se derivan del trabajo desarrollado en la misma.

B.1. Capítulos de libros

- E. Kovacs, L. Sanchez, **J. Lanza**, J. Hoebeke, M. G. Genet, M. Bauer, R. L. Olsen, M. Ghader, H. Thuvesson y L. Muñoz, “PN networking”, inglés, en *My Personal Adaptive Global NET (MAGNET)*, 1st, ép. Signals and Communication Technology. Springer Publishing Company, Inc., 2010, cap. 3, págs. 75-134, ISBN: 9789048134366, 978-90-481-3437-3.
- J. Zidbeck, L. Sanchez, K. Ahola, M. Alutoin, M. Bauer, S. Bessler, M. G. Genet, J. Hoebeke, **J. Lanza**, I. Moerman, R. L. Olsen, J. J. Pallares y J. Zeiss, “PN Platforms”, inglés, en *My Personal Adaptive Global NET (MAGNET)*, 1st, ép. Signals and Communication Technology. Springer Publishing Company, Inc., 2010, cap. 7, págs. 337-407, ISBN: 9789048134366, 978-90-481-3437-3.

B.2. Revistas internacionales

- L. Sánchez, I. Elicegui, J. Cuesta, L. Muñoz y **J. Lanza**, “Integration of Utilities Infrastructures in a Future Internet Enabled Smart City Framework”, *Sensors*, vol. 13, n.º 11, págs. 14 438-14 465, 2013, ISSN: 1424-8220.
- L. Sánchez, **J. Lanza**, L. Muñoz y K. A. M. Alutoin, “Securing the Communication in Private Heterogeneous Mobile Ad hoc Networks”, *Wireless Personal Communications*, vol. 52, n.º 2, págs. 393-409, 2010, ISSN: 0929-6212.
- L. Sánchez, **J. Lanza** y L. Muñoz, “Optimisation of dynamic interface selection mechanisms on multi-radio devices in ad hoc networks”, *Electronics Letters*, vol. 45, n.º 11, págs. 558-559, mayo de 2009, ISSN: 0013-5194.

- L. Sánchez, **J. Lanza** y L. Muñoz, “Extending Private Personal Area Networks to Personal Network Federations in heterogeneous ad-hoc scenarios”, *Special issue on Personal Networks of Teletronikk journal*, vol. 103, n.º 1–2007, págs. 34-44, feb. de 2007, ISSN: 0085-7130.
- D. M. Kyriazanos, M. Argyropoulos, L. Sánchez, **J. Lanza**, M. Alutoin, J. Hoebeke y C. Z. Patrikakis, “Overview of a Personal Network Prototype”, *IEC Annual Review of Communications*, vol. 59, 2006.
- L. Sánchez, **J. Lanza** y L. Muñoz, “Experimental Assessment of a Cross-Layer Solution for TCP/IP Traffic Optimization on Heterogeneous Personal Networking Environments”, *Lecture Notes in Computer Science*, vol. 4217, págs. 284-296, sep. de 2006, ISSN: 0302-9743.

B.3. Conferencias internacionales

- J. Rico, B. Cendon, **J. Lanza** y J. Valiño, “Bringing IoT to Hospital Logistics Systems Demonstrating the concept”, en *Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE*, abr. de 2012, págs. 196-201.
- L. Sanchez, **J. Lanza** y L. Muñoz, “Energy Efficiency of Dynamic Interface Selection Mechanisms in Wireless Ad-Hoc Networks”, English, en *Mobile Networks and Management*, ép. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, K. Pentikousis, R. Agüero, M. García-Arranz y S. Papavassiliou, eds., vol. 68, Springer Berlin Heidelberg, 2011, págs. 188-197, ISBN: 978-3-642-21443-1.
- **J. Lanza**, L. Sánchez y L. Muñoz, “Experimental Comparison of Two Solutions for Securing Heterogeneous Ad-Hoc Network Communications”, en *11th International Symposium on Wireless Personal Multimedia Communications*, Lapland, Finland, sep. de 2008.
- L. Sánchez, **J. Lanza**, J. Hoebeke, I. Moerman, M. Alutoin, K. Ahola, J. J. Pallares, M. G. Genet, M. Bauer y J. Zeiss, “Assessing Personal Networks on a pan-European Testbed”, en *ICT Mobile and Wireless Communications Summit 2008*, Stockholm, Sweden, 2008.
- R. Olsen, M. Bauer, L. Sanchez y **J. Lanza**, “Self Organisation of Context Agents in Personal Networks and Federations”, en *10th International Symposium on Wireless Personal Multimedia Communications*, Jaipur, India, jun. de 2007.
- L. Sánchez, **J. Lanza** y L. Muñoz, “Federating Personal Networks over Heterogeneous Ad hoc Scenarios”, en *12th IFIP International Conference on Personal Wireless Communications*, S. I. Series, ed., vol. 245, Prague, Czech Republic, sep. de 2007, págs. 38-53.

- L. Sánchez, **J. Lanza**, J. Rico y L. Muñoz, “Implementation of a Vertical Handover Solution for Coexisting Ad-hoc Multihop and Infrastructure Access Networks based on IEEE 802.11”, en *7th International Workshop on Applications and Services in Wireless Networks*, Santander, Spain, mayo de 2007, págs. 15-21, ISBN: 978-84-690-5727-8.
- M. Bauer, R. L. Olsen, M. Jacobsson, L. Sánchez, **J. Lanza**, M. Imine y N. Prasad, “Context Management Framework for MAGNET Beyond”, en *15th IST Mobile & Wireless Summit Communications Summit*, Mykonos, Greece, jun. de 2006.
- M. Ghader, R. L. O. Olsen, V. Prasad, M. Jacobsson, L. Sánchez, **J. Lanza**, W. Louati, M. Girod Genet, D. Zeghlache y R. Tafazolli, “Service Discovery in Personal Networks: design, implementation and analysis”, en *15th IST Mobile & Wireless Summit Communications Summit*, Mykonos, Greece, jun. de 2006.
- J. Hoebeke, G. Holderbeke, I. Moerman, W. Louati, W. Louati, M. Girod Genet, D. Zeghlache, L. Sánchez, **J. Lanza**, M. Alutoin, K. Ahola, S. Lehtonen y J. Jaen Pallares, “Personal Networks: From concept to a demonstrator”, en *15th IST Mobile & Wireless Summit Communications Summit*, Mykonos, Greece, jun. de 2006.
- **J. Lanza**, L. Sánchez y L. Muñoz, “Cluster Head Selection and Maintenance over Heterogeneous Mobile Wireless Personal Area Networks. an experimental approach”, en *9th International Symposium on Wireless Personal Multimedia Communications*, San Diego (CA), USA, sep. de 2006.
- **J. Lanza**, L. Sánchez y L. Muñoz, “Performance Evaluation of a Cross-layer based Wireless Interface Dynamic Selection on WPAN/WLAN Heterogeneous Environments: An Experimental Approach”, en *6th International Workshop on Applications and Services in Wireless Networks*, Berlin, Germany, mayo de 2006, págs. 139-146, ISBN: 3-8167-7111-4.
- L. Sánchez, **J. Lanza**, M. Bauer, R. L. Olsen y M. Girod Genet, “A Generic Context Management Framework for Personal Networking Environments”, en *The Third Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, San Jose (CA), USA, jul. de 2006, págs. 1-8, ISBN: 0-7803-9792-4.
- M. Alutoin, K. Ahola, S. Lehtonen, L. Sánchez, **J. Lanza**, J. Hoebeke, G. Holderbeke, I. Moerman, M. G. Genet y W. Louati, “Self-organisation and mobility in Personal Networks”, en *8th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, sep. de 2005, págs. 318-322, ISBN: 87-90834-82-8.
- M. Alutoin, S. Lehtonen, J. Hoebeke, G. Holderbeke, I. Moerman, L. Sánchez, **J. Lanza**, D. Zeghlache y W. Louati, “Towards Self-organising Personal Networks”, en *1st ACM Workshop on Dynamic Interconnection of Networks*, Cologne, Germany, sep. de 2005, págs. 12-16, ISBN: 1-59593-144-9.
- L. Sánchez, **J. Lanza** y L. Muñoz, “Self-Configuring Private Personal Area Networks: The first stage towards Personal Networking”, en *8th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, sep. de 2005, págs. 1983-1987, ISBN: 87-90834-82-8.

- L. Sánchez, **J. Lanza**, L. Muñoz y J. Perez, “Enabling Secure Communications over Heterogeneous Air Interfaces: Building Private Personal Area Networks”, en *8th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, sep. de 2005, págs. 1963-1967, ISBN: 87-90834-82-8.

B.4. Conferencias nacionales

- L. Sánchez, **J. Lanza** y L. Muñoz, “Eficiencia Energética de un Mecanismo de Selección Dinámica de Interfaces en Redes Ad-hoc Inalámbricas”, en *X Jornadas de Ingeniería Telemática*, Santander, Spain, sep. de 2011, págs. 245-250, ISBN: 978-84-694-5948-5.
- L. Sánchez, **J. Lanza**, J. Choque, L. Muñoz y D. González, “Arquitectura de una Entidad Middleware para la Gestión Cognitiva de las Comunicaciones en Terminales Multiradio”, en *IX Jornadas de Ingeniería Telemática*, Valladolid, Spain, sep. de 2010, ISBN: 978-84-693-5398-1.
- L. Sánchez, **J. Lanza**, L. Muñoz y J. Rico, “Redes Personales: la implementación del concepto”, en *XVII Jornadas TELECOM I+D*, Valencia, Spain, feb. de 2007.
- R. Agüero, L. Muñoz, J. Choque, L. Sánchez y **J. Lanza**, “Estudio experimental de los protocolos IP en redes inalámbricas multi-salto basadas en el protocolo DSR”, en *V Jornadas de Ingeniería Telemática*, Vigo, Spain, sep. de 2005, págs. 217-224, ISBN: 84-8408-346-2.
- **J. Lanza**, R. Beivide y R. Menendez, “Plataformas distribuidas para calculo paralelo”, en *XI Jornadas de Paralelismo*, Granada, Spain, sep. de 2000, ISBN: 87-90834-82-8.

B.5. Solicitudes de patentes

- J. Jaen-Pallares, L. Sánchez, **J. Lanza** y L. Muñoz, *Method for distributing a Certificate Revocation List in a network*, Solicitud de patente 08167197.6, oct. de 2008.
- L. Muñoz, **J. Lanza**, O. Blanco, J. A. Torrero, L. Rodriguez, O. Blanco, P. Real y M. Gorricho, *Método de autenticación de usuarios para acceso a aplicaciones informáticas y firma de documentos electrónicos a través del teléfono móvil*, Solicitud de patente P200302370, oct. de 2003.

B.6. Ponencias y cursos

- **J. Lanza**, “Host Card Emulation: Moving smartcards to the cloud”, en *II International Congress University Smart Card*, Murcia, Spain, abr. de 2014.
- **J. Lanza**, “Public transport and University Smart Card”, en *II Internacional Congress University Smart Card*, Murcia, Spain, abr. de 2014.
- **J. Lanza**, “Smart Cards Fundamentals and Beyond”, ERASMUS IP 2014, University of Cantabria, Santander, Spain, mayo de 2014.

- **J. Lanza**, “University of Cantabria - Use Case Beyond just a Campus Card”, en *12th European Campus Card Conference*, Santander, Spain, mayo de 2014.
- **J. Lanza**, “New Challenges on Campus Smart Cards”, en *11th European Campus Card Conference*, Porto, Portugal, mayo de 2013.
- **J. Lanza**, “TUI santander: a University Smartcard Standard”, en *I Internacional Congress University Smart Card*, Murcia, Spain, mayo de 2013.
- **J. Lanza**, “Las Smart Cities y el Comercio”, en *Jornada Sociedad, Ciudad y Comercio*, Burgos, Spain, nov. de 2012.
- **J. Lanza**, “The Smart Card in the Smart University”, en *10th European Campus Card Conference*, Lund, Sweden, mayo de 2012.
- **J. Lanza**, “Santander Universities Smart Card: The Prepaid Card”, en *8th European Campus Card Conference*, Waterford, Ireland, mayo de 2010.
- **J. Lanza** y V. Prior, “Identificación Digital. Experiencia en las universidades”, en *El gobierno electrónico de la universidad*, Universidad Internacional de Andalucía, Tetuán, Marrocco, jul. de 2006.
- L. Muñoz, L. Sánchez, **J. Lanza**, M. Alutoin, S. Lehtonen, D. Zeghlache, M. Girot Genet, W. Louati, I. Moerman, J. Hoebeke, G. Holderbeke, M. Ghader y M. Jacobsson, “A proposal for self-organizing Personal Networks”, en *WWRF meeting 15*, Paris, France, dic. de 2005.
- **J. Lanza**, “Smart Cards and Digital Signature”, en *2nd European Campus Card Conference*, London, Great Britain, jun. de 2004.
- **J. Lanza**, “Seguridad en tarjetas inteligentes”, en *Seguridad en Redes Informáticas y de Telecomunicaciones*, Cursos de Verano de la Universidad de Cantabria, Laredo, Spain, ago. de 2003.
- **J. Lanza**, “Tarjetas Inteligentes. Un soporte seguro”, en *NeoCom*, Asociación de Estudiantes de Telecomunicaciones de la Universidad de Zaragoza, Zaragoza, Spain, dic. de 2003, ISBN: 84-7653-824-3.
- **J. Lanza** y L. Muñoz, “The WAL: A performance enhancing proxy for heterogeneous access”, en *Workshop on Internet Usage over 2.5G and 3G*, Barcelona, Spain, mar. de 2003, págs. 134-143, ISBN: 84-7653-824-3.
- **J. Lanza** y O. Blanco, “Java Card Programming: The practical experience of the University of Cantabria”, en *1st European Campus Card Conference*, Waterford, Ireland, jun. de 2002.

B.7. Documentos científico-técnicos

- All WP2 Partners, “Second federation architecture”, Federation for FIRE, Deliverable 2.4, mar. de 2014.
- M. Sawyer, G. Francis, I. Panourgias, P. Sotres, **J. Lanza**, D. Margery, J. Lefeuvre y F. Schreiner, “Report on first cycle developments of the services and applications community”, Federation for FIRE, Deliverable 4.3, mar. de 2014.
- F. Lobillo, M. Sawyer, G. Francis, **J. Lanza**, P. Sotres, B. Bochow, M. Smirnov, B. Vermeulen y D. Margery, “Second input from the Services and Applications community to the architecture”, Federation for FIRE, Deliverable 4.2, nov. de 2013.
- O. Mehani, G. Jourjon, Y. Al-Hazmi, W. Vandenberghe, D. Stavropoulos, **J. Lanza**, K. Choumas, L. Sanchez y P. Sotres, “Detailed specifications for first cycle ready”, Federation for FIRE, Deliverable 6.1, mar. de 2013.
- J. V. Ooteghem, B. Naudts, W. Vandenberghe, B. Vermeulen, S. Bouckaert, S. Taylor, P. Grace, F. Lobillo, J. Martrat, L. Muñoz, **J. Lanza**, P. Sotres y M. Sawyer, “First Sustainability Plan”, Federation for FIRE, Deliverable 2.3, jul. de 2013.
- F. Lobillo, M. Sawyer, S. Taylor, K. Kavoussanakis, **J. Lanza**, L. Muñoz, P. Sortres y D. Margery, “First input from community to architecture”, Federation for FIRE, Deliverable 4.1, nov. de 2012.
- B. Vermeulen, W. Vandenberghe, T. Leonard, T. Friedman, F. Schreiner, K. Kavoussanakis, M. Ott, F. L. Vilela, P. Sotres y **J. Lanza**, “First federation architecture”, Federation for FIRE, Deliverable 2.1, dic. de 2012.
- AT4 Wireless, Caja Navarra, Telefónica I+D, Telvent, Universidad de Málaga, **Universidad de Cantabria** y WorldNet21, “Análisis de la seguridad y confidencialidad para aplicaciones críticas”, Proyecto CENIT mIO!, Entregable 5.3.3, 2011.
- AT4 wireless, Inabensa, **Universidad de Cantabria** y Universidad de Vigo, “Soporte de publicación de interfaces de acceso proporcionadas por la infraestructura o por dispositivos de terceros”, Proyecto CENIT mIO!, Entregable 6.5.6, dic. de 2011.
- AT4 wireless, Inabensa, **Universidad de Cantabria**, Universidad Politécnica de Cartagena y Centro Tecnológico de Telecomunicaciones de Cataluña, “Soporte de trasposos de tecnologías de comunicación en redes 3G y WLAN. Aspectos de admisión y QoS”, Proyecto CENIT mIO!, Entregable 6.5.6, dic. de 2011.
- Cemitec, Telefónica I+D, Telvent, Treelogic y **Universidad de Cantabria**, “Activos Experimentales”, Proyecto CENIT mIO!, Entregable 4.7.2, dic. de 2011.
- Inabensa, AT4 Wireless, Universidad de Vigo y **Universidad de Cantabria**, “Especificación, diseño y selección de los sistemas de comunicación con las interfaces de acceso en función del servicio”, Proyecto CENIT mIO!, Entregable 6.1.3, 2011.

- Inabensa, AT4 Wireless, Universidad de Vigo y **Universidad de Cantabria**, “Estudio y definición de modelos de seguridad para las comunicaciones con los interfaces que proporcionan los dispositivos de terceros”, Proyecto CENIT mIO!, Entregable 6.1.4, 2011.
- Inabensa, AT4 wireless, Worldnet21, Centro Tecnológico de Telecomunicaciones de Cataluña, Universidad de Málaga, **Universidad de Cantabria** y Universidad de Castilla La Mancha, “Técnicas de cognitive radio, que permiten la compartición del espectro entre distintas comunicaciones inalámbricas”, Proyecto CENIT mIO!, Entregable 6.2.7, 2011.
- Telefónica I+D y **Universidad de Cantabria**, “Configurador de parámetros de red empleando tecnologías NFC y tarjeta inteligente”, Proyecto CENIT mIO!, Entregable - Activo Experimental 4.5.3_AE_5, ene. de 2011.
- Telefónica I+D y **Universidad de Cantabria**, “Estudio de casos de uso en entornos de distribución”, Proyecto CENIT mIO!, Entregable 4.5.3, dic. de 2011.
- Telefónica I+D y **Universidad de Cantabria**, “Estudio tecnológico para el modelado y desarrollo de servicios de retail”, Proyecto CENIT mIO!, Entregable 4.5.2, jun. de 2011.
- Telefónica I+D, **Universidad de Cantabria**, Telvent, Treelogic, Cemitec y WorldNet 21, “Metodologías de desarrollo de servicios en entornos inteligentes”, Proyecto CENIT mIO!, Entregable 4.6.2, dic. de 2011.
- Telvent, ECSC, Robotiker, Telefónica I+D, Treelogic y **Universidad de Cantabria**, “Mecanismos para la orquestación de servicios”, Proyecto CENIT mIO!, Entregable 4.7.1, ene. de 2011.
- Worldnet21, Telvent, Telefónica I+D, **Universidad de Cantabria**, AT4 wireless, Universidad de Málaga, Universidad de Castilla La Mancha, Universidad Rey Juan Carlos, Inabensa y Universidad de Vigo, “Análisis de topologías, arquitecturas y tecnologías de interconexión en entornos inteligentes con gran número de elementos distribuidos”, Proyecto CENIT mIO!, Entregable 5.3.5, dic. de 2011.
- AT4 Wireless, Inabensa, Robotiker, Telefónica I+D, Telvent, Universidad Cantabria, Universidad de Vigo, Universidad Rey Juan Carlos y Worldnet21, “Definición de técnicas de nivel físico para el posicionamiento de alta precisión en exteriores e interiores”, Proyecto CENIT mIO!, Entregable 5.2.1, feb. de 2010.
- AT4 Wireless, Inabensa, Robotiker, Telefónica I+D, Telvent, Universidad de Vigo, Universidad Rey Juan Carlos, **Universidad de Cantabria** y Worldnet21, “Modelos y métodos de integración de dispositivos de distinta naturaleza”, Proyecto CENIT mIO!, Entregable 5.2.2, feb. de 2010.
- AT4 wireless, Inabensa, Robotiker, Telefónica I+D, Telvent, **Universidad de Cantabria**, Universidad de Vigo, Universidad Rey Juan Carlos y WorldNet21, “Especificación de estrategias para el roaming de servicios entre diferentes contextos y redes”, Proyecto CENIT mIO!, Entregable 5.2.4, feb. de 2010.

- AT4 wireless, Inabensa y **Universidad de Cantabria**, “Análisis de los requisitos de gestión en función de los servicios en movilidad”, Proyecto CENIT mIO!, Entregable 6.5.2, ene. de 2010.
- AT4 wireless, Inabensa, **Universidad de Cantabria**, Universidad Politécnica de Cartagena, Universidad de Vigo y Centro Tecnológico de Telecomunicaciones de Cataluña, “Nuevos Modelos, Técnicas y Mecanismos de gestión de las comunicaciones”, Proyecto CENIT mIO!, Entregable 6.5.3, ene. de 2010.
- AT4 Wireless, Robotiker, Telefónica I+D, Telvent, **Universidad de Cantabria**, Universidad de Castilla la Mancha, Universidad de Málaga, Universidad Rey Juan Carlos y Worldnet21, “Análisis de sistemas de sensorización activos y balizamiento de pequeño tamaño y muy bajo consumo para un despliegue masivo de infraestructura de entornos inteligentes. Sensores y elementos inteligentes interconectados”, Proyecto CENIT mIO!, Entregable 5.3.4, nov. de 2010.
- AT4 Wireless, Universidad de Málaga y **Universidad de Cantabria**, “Tendencias Tecnológicas en los Terminales Móviles”, Proyecto CENIT mIO!, Entregable 6.4.1, jun. de 2010.
- Inabensa, AT4 Wireless, Universidad de Málaga, Universidad de Vigo y **Universidad de Cantabria**, “Investigación en comunicaciones integradas en los dispositivos de acceso. Requisitos de los dispositivos de acceso para la integración. Análisis de requisitos de la comunicación entre dispositivos de acceso y terminales móviles”, Proyecto CENIT mIO!, Entregable 6.1.2, feb. de 2010.
- Inabensa, AT4 Wireless, Worldnet21, Universidad de Vigo, Universidad de Málaga, **Universidad de Cantabria** y Universidad Rey Juan Carlos, “Mejora en las tecnologías de comunicación entre el usuario y el entorno inteligente mediante técnicas de colaboración entre capas (cross-layer)”, Proyecto CENIT mIO!, Entregable 6.2.5, feb. de 2010.
- Telefónica I+D, **Universidad de Cantabria**, Telvent, Robotiker-Tecnalia, Caja Navarra y CEMITEC, “Estudio de Disponibilidad de Tecnologías de Movilidad”, Proyecto CENIT mIO!, Entregable 4.1.2, feb. de 2010.
- AT4 Wireless, Inabensa, Robotiker-Tecnalia, Telefónica I+D, Telvent, **Universidad de Cantabria**, Universidad de Málaga, Universidad de Vigo, Universidad Rey Juan Carlos y WorldNet21, “Análisis de interacción usuario-entorno en diferentes ambientes físicos”, Proyecto CENIT mIO!, Entregable 5.3.1, nov. de 2009.
- AT4 wireless, Inabensa, **Universidad de Cantabria**, Universidad de Vigo y Centro Tecnológico de Telecomunicaciones de Cataluña, “Tendencias en gestión de comunicaciones”, Proyecto CENIT mIO!, Entregable 6.5.1, mar. de 2009.
- AT4 Wireless, **Universidad de Cantabria**, Universidad de Málaga, Universidad Rey Juan Carlos, WorldNet21, Inabensa, CTTC, TB Solutions y Robotiker, “Investigación y evaluación de las tecnologías MAN y sus capacidades para proveer servicios ubicuos y en movilidad”, Proyecto CENIT mIO!, Entregable 6.3.1, mar. de 2009.

- Inabensa, AT4 Wireless, Worldnet21, Universidad de Vigo, **Universidad de Cantabria**, Universidad de Málaga y Universidad Rey Juan Carlos, “Análisis de requisitos de conexión entre el usuario y el entorno inteligente proporcionando servicios personalizados en movilidad”, Proyecto CENIT mIO!, Entregable 6.2.4, sep. de 2009.
- Inabensa, AT4 Wireless, Worldnet21, Universidad Politécnica de Cartagena, Universidad de Málaga, **Universidad de Cantabria** y Universidad Rey Juan Carlos, “Investigación en esquemas de acceso al medio de las tecnologías de comunicación entre el usuario y el entorno inteligente, para mejorar la eficiencia energética”, Proyecto CENIT mIO!, Entregable 6.2.2, sep. de 2009.
- Inabensa, AT4 Wireless, Worldnet21, Universidad de Vigo, Universidad de Málaga, **Universidad de Cantabria** y Universidad Rey Juan Carlos, “Investigación en la selección óptima de la tecnología de comunicación entre el usuario y el entorno inteligente en función del consumo energético y del ancho de banda requerido”, Proyecto CENIT mIO!, Entregable 6.2.3, sep. de 2009.
- Inabensa, Universidad de Vigo, AT4 Wireless, **Universidad de Cantabria**, Universidad de Málaga, Universidad Rey Juan Carlos y WorldNet21, “Investigación en tecnologías y elementos de interconexión entre el usuario y el entorno inteligente”, Proyecto CENIT mIO!, Entregable 6.2.1, mar. de 2009.
- Inabensa, Universidad Politécnica de Cartagena, AT4 Wireless, **Universidad de Cantabria** y Universidad de Málaga, “Investigación en comunicaciones inalámbricas de corto alcance. Estado del arte. Caracterización y evaluación de estas tecnologías en el contexto del proyecto”, Proyecto CENIT mIO!, Entregable 6.1.1, mar. de 2009.
- Telefónica I+D, Telvent, Robotiker, **Universidad de Cantabria**, Caja Navarra, CEMITEC, WorldNet21 y Treelogic, “Especificación de requisitos de un entorno de creación de servicios inteligentes”, Proyecto CENIT mIO!, Entregable 4.6.1, nov. de 2009.
- Telefónica I+D, Telvent, Robotiker, **Universidad de Cantabria**, Caja Navarra y CEMITEC, “Estado del Arte de Tecnologías de Prestación de Servicios en Movilidad”, Proyecto CENIT mIO!, Entregable 4.1.1, mar. de 2009.
- Telefónica I+D, Telvent, Robotiker, **Universidad de Cantabria**, Caja Navarra y CEMITEC, “Estudio de las Tendencias en Tecnologías de Servicios de Distribución Comercial”, Proyecto CENIT mIO!, Entregable 4.5.1, mar. de 2009.
- Telefónica I+D y **Universidad de Cantabria**, “Sistema de autenticación y pagos basado en NFC en modo P2P”, Proyecto CENIT mIO!, Entregable - Activo Experimental 4.5.3_AE_3, jun. de 2009.
- Telvent, AT4 Wireless, Inabensa, Robotiker, Telefónica I+D, **Universidad de Cantabria**, Universidad de Málaga, Universidad de Vigo, Universidad Rey Juan Carlos y WorldNet21, “Análisis de escenarios de implementación en entornos cerrados”, Proyecto CENIT mIO!, Entregable 5.1.2, mar. de 2009.

- Telvent, AT4 wireless, Robotiker, Telefónica I+D, **Universidad de Cantabria**, Universidad de Málaga, Universidad Rey Juan Carlos y WorldNet21, “Análisis de escenarios de implementación en entornos abiertos (ciudad)”, Proyecto CENIT mIO!, Entregable 5.1.1, mar. de 2009.
- M. G. Genet, D. Zeghlache, M. Ghader, D. Kraft, M. Bauer, E. Kovacs, J. Hoebeke, R. L. Olsen, M. Jacobsson, H. Thuvesson, J. Zeiss, S. Bessler, L. Sanchez y **J. Lanza**, “Specifications of interfaces and interworking between PN networking architecture and service architectures”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 2.2.1, feb. de 2008.
- M. Jacobsson, I. Niemegeers, Y. Gu, T. Ahola, K. Ahola, M. Alutoin, M. Bauer, M. Girod-Genet, M. Ghader, A. Gouya, J. Hoebeke, G. Holderbeke, J. Jaen-Pallares, U. Javaid, P. Karlsson, **J. Lanza**, W. Louati, W. Louati, D.-E. Meddour, I. Moerman, R. L. Olsen, V. Prasad, L. Sanchez, J. Stoter, H. Thuvesson y D. Zeghlache, “PN secure networking frameworks, solutions and performance”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 2.3.2, jun. de 2008.
- L. Biard, D. Noguét, N. Sortur, A. Saxena, M. Shunmugam, L. Sanchez, **J. Lanza**, M. Saavela y K. Ahola, “Complete MAGNET system platform towards Pilot Services”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 6.4.1, oct. de 2007.
- J. Hoebeke, I. Moerman, R. De Spiegelaere, S. Charfi, W. Louati, M. Girod-Genet, L. Sanchez, **J. Lanza**, J. Rico, T. Ahola, K. Ahola, M. Alutoin y J. Jaen-Pallares, “Performance and Functionality Analysis of the PN Platform”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 6.3.2, dic. de 2007.
- J. Jaen Pallares, H. Affi, M. Argyropoulos, M. Bauer, S. Bessler, M. Girod-Genet, D. Kyriazanos, W. Louati, S. Mirzadeh, N. Prasad, J. Stoter, J. Zeiss, **J. Lanza** y L. Sanchez, “Selections and Implementation of protocols and solutions in the view of PN-Platform”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 4.1.2, feb. de 2007.
- L. Sanchez, **J. Lanza**, K. Ahola, M. Alutoin, R. De Spiegelaere, J. Jaen-Pallares, S. Charfi y M. Girod-Genet, “PN related platform towards Pilot Services”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 6.3.1, dic. de 2007.
- J. Zidbeck, T. Ahola, K. Ahola, M. Alutoin, M. Girod-Genet, J. Hoebeke, G. Holderbeke, J. Jaen-Pallares, **J. Lanza**, S. Charfi, I. Moerman, R. L. Olsen, L. Sanchez, D. Zeghlache y J. Zeiss, “MAGNET system secure networking components implementation”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 6.2.1, mayo de 2007.
- J. Zidbeck, T. Ahola, K. Ahola, M. Alutoin, M. Girod-Genet, J. Hoebeke, G. Holderbeke, J. Jaen-Pallares, **J. Lanza**, S. Charfi, I. Moerman, R. L. Olsen, L. Sanchez, D. Zeghlache y J. Zeiss, “PN networking and security components conformance report”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 6.1.1, jun. de 2007.

- M. Bauer, **J. Lanza**, L. Sanchez y col., “Final interface specification for context aware components”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Internal Report 2.1.1, sep. de 2006.
- Y. Durand, D. Lattard, D. Mottier, T. Van Leeuwen, **J. Lanza**, A. Acha, L. Sanchez y E. Gomez, “Platform performance and architecture requirements”, WISQUAS (Wireless Systems providing high QUALity Services), Deliverable 4.1, abr. de 2006.
- E. Gomez, L. Sanchez, **J. Lanza**, L. Arnaiz, L. Muñoz, C. Desset, S. Simoens, S. Gunaratne, D. Ktenas y S. Mayrargue, “Efficient system simulation and behavioural modelling at all layers, with cross-layer metric modelling”, WISQUAS (Wireless Systems providing high QUALity Services), Deliverable 1.2, oct. de 2006.
- M. Jacobsson, M. Alutoin, M. Bauer, M. G. Genet, M. Ghader, A. Gouya, J. Hoebeke, G. Holderbeke, J. Jaen-Pallares, U. Javaid, P. Karlsson, **J. Lanza**, W. Louati, W. Louati, D.-E. Meddour, I. Moerman, R. L. Olsen, V. Prasad, L. Sanchez, J. Stoter, H. Thuvesson y D. Zeghlache, “Specification of PN networking and security components”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 2.3.1, dic. de 2006.
- E. Kovacs, **J. Lanza**, L. Sanchez, K. Ahola, M. Jacobsson, M. Alutoin y M. B. et al., “MAGNET System Specification”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Deliverable 1.1.1, oct. de 2006.
- L. Peters, T. Van Leeuwen, I. Moerman, A. Acha, L. Sanchez, **J. Lanza**, E. Gomez e Y. Presumey, “Handover solutions for intra and inter system service continuity”, WISQUAS (Wireless Systems providing high QUALity Services), Deliverable 3.2, mar. de 2006.
- L. Sanchez, **J. Lanza** y col., “Preliminary interface specification for context aware and L2/L3 interfaces”, MAGNET Beyond (My personal Adaptive Global NET y Beyond), Milestone 2.1.1, abr. de 2006.
- P. Balamuralidhar, N. Marthur, M. De Sanctis, L. Sanchez, **J. Lanza**, J. Perez, G. P. Perrucci, K. Schoo, J. Rodriguez, M. Presser, D. Dahlhaus y C. Peel, “MAC/RRM Schemes for WPAN (Update D3.3.2a)”, MAGNET (My personal Adaptive Global NET), Deliverable 3.3.2b, dic. de 2005.
- S. Lehtonen, M. Alutoin, K. Ahola, L. Sanchez, **J. Lanza**, L. Muñoz, W. Louati, W. Louati, M. Girod Genet, D. Zeghlache, G. Holderbeke, J. Hoebeke, J. Oksa y A. Pietiläinen, “Early Prototype Demonstration based on Active Engine and PAN/PN based to PDAs/Laptops”, MAGNET (My personal Adaptive Global NET), Deliverable 2.5.3, oct. de 2005.
- R. L. Olsen, M. Ghader, M. Girod Genet, W. Louati, D. Zeghlache, H. P. Schwefel, L. Gavrilovska, M. Duspiva, M. Wellens, M. Petrova, L. Sanchez y **J. Lanza**, “Service, Resource and Context Discovery system specification”, MAGNET (My personal Adaptive Global NET), Deliverable 2.2.3, dic. de 2005.

- L. Sanchez, **J. Lanza**, L. Muñoz, J. Hoebeke, G. Holderbeke, I. Moerman, W. Louati, W. Louati, M. Girod Genet, D. Zeghlache, K. Ahola, M. Alutoin y S. Lehtonen, “Definition of full PAN/PN Network Terminal Prototyping System”, MAGNET (My personal Adaptive Global NET), Deliverable 2.5.2, dic. de 2005.
- M. De Sanctis, P. Giorgi, M. Presser, I. Ghauri, C. Peel, J. Perez, **J. Lanza**, L. Sanchez, P. Luis Muñoz Balamuralidhar, H. Choi y F. Fitzek, “MAC/RRM Schemes for WPAN”, MAGNET (My personal Adaptive Global NET), Deliverable 3.3.2a, oct. de 2004.
- M. Ghader, R. L. Olsen, L. Sanchez, **J. Lanza**, L. Muñoz, J. Hoebeke, I. Moerman, M. Petrova, M. Wellens, M. Girod Genet, W. Louati, K. Masmoudi, D. Zeghlache, N. Köstering, S. Lehtonen y R. Tafazolli, “Resource and Service Discovery: PN Solutions”, MAGNET (My personal Adaptive Global NET), Deliverable 2.2.1, dic. de 2004.
- M. Petrova, M. Jacobson, S. Oosthoek, J. Hoebeke, I. Moerman, H. Afifi, D. Zeghlache, L. Muñoz, L. Sanchez, **J. Lanza**, M. Latvala, K. Nyberg, D. Sisalem, M. Presser, M. Ghader y S. Mirzadeh, “Conceptual Secure PN Architecture”, MAGNET (My personal Adaptive Global NET), Deliverable 2.1.1, dic. de 2004.
- L. Sanchez, V. Gutierrez, O. Blanco, R. Agüero, R. San Juan, J. Choque, **J. Lanza**, J. A. Irastorza, L. Muñoz, Y. Liu, L. Gavrilovska, H. P. Schwefel, E. Puig, A. Markopoulos, J. Spanoudakis, S. Schallenburger y S. Velentzas, “Link layer techniques in an ad-hoc WPAN environment”, PACWOMAN (Power Aware Communications for Wireless OptiMised personal Area Networks), Deliverable 5.3, sep. de 2004.
- L. Sanchez, **J. Lanza**, L. Muñoz, D. Zeghlache, W. Louati, W. Louati, I. Moerman, S. Pönkänen, S. Lehtonen, N. Köstering, S. Heemstra de Groot y M. Jacobson, “Prototype concepts of a PAN/PN terminal and infrastructure network support”, MAGNET (My personal Adaptive Global NET), Deliverable 2.5.1, dic. de 2004.

UNIVERSIDAD DE CANTABRIA

DEPARTAMENTO DE INGENIERÍA DE COMUNICACIONES



THESIS SUMMARY

Contribution to the design and evaluation of Cognitive Personal Networks

Author: *Jorge Lanza Calderón*

Director: *Luis Muñoz*

Santander, July 2014

Abstract

It is now more than fifty years since the first seeds were sown of what is now known as the Information and Communications Society. Historical vision allows us to state without any doubt that during this period much of the work done in terms of research, development and innovation efforts has been aimed at consolidating a massive, worldwide communications infrastructure that firstly made communication between people possible and later extended this to machines in their widest sense.

Early this century that paradigm shifted toward the individual, promoting new technologies and services that facilitated the communication of myriad user-centred devices in order to acquire, process and decide the appropriate action based on different considerations, such as the context or privacy. Thus, the concept of personal area network appeared which expanded, under different initiatives, to personal network and personal network federation. Terms such as heterogeneity and scalability are intrinsic to the concept of federation infrastructure as is demonstrated in this thesis, which provides architectural solutions unified for this purpose.

Previously, based on a sufficiently large set of usage cases, functional requirements were identified that specifically characterize the needs of personal networks and their federation. In order to elucidate the mechanisms that have been proposed to fulfil these requirements, a detailed study of the state-of-the-art has been carried out, both in relation to standardization activities and to significant international projects.

Once the requirements have been established, the concept of Personal Network (PN) is defined. Its architecture is based on three layers;: an abstraction layer at the connectivity level, another at network level and another at service level. In the connectivity level abstraction layer, the direct interconnection among user devices is examined. In order to address heterogeneity in terms of medium access technologies, an Universal Convergence Layer (UCL) is defined, which can intelligently manage the access interfaces and isolate the upper communication layers from the underlying complexity. The network level abstraction layer deals with the mechanisms for grouping and communication of the nodes in a PN, on which the service's data exchange is based. The service level abstraction layer provides a distributed management platform that supports the creation, publication, discovery and provision of services.

Orthogonally to the above three layers, another layer was proposed for the acquisition, management and delivery of the user context. The information flow through this layer will allow the other three to adapt their operation based on the specific user needs, the environment and other PNs wishing to interact with it.

As can also be understood from the analysis of the usage cases, security in the PN plays a key role in motivating users in the use of this type of infrastructure. Thus, to ensure privacy, authenticity and non-repudiation of communications, strategies are conceived and designed to make the PN a secure network. Supported by the existing ownership relationship between user devices and the users themselves, procedures are established for generating a bilateral trust relationship between nodes of the PN. This bond is propagated throughout the different abstraction layers, ensuring the secure exchange of information within the PN.

Once the PN had been analysed from all levels as an autonomous entity, the PN was expanded with the concept of Personal Networks Federation as well as with a global design proposal of its associated architecture. Considering the PN-F as the aggregation of PNs that share resources, new entities were identified supporting added functionalities or extending those originating in the PNs in order to integrate them into the PN-F framework. The approach follows two approximations: one that considers the PN-F as an aggregation at the network level on which all types of resources are shared and another in which the aggregation is performed only at service level.

As an extension to the specification and design work described in the first five chapters of this thesis, Chapter 6 is intended to validate the different solutions proposed in field environments. This required a demonstrator distributed in different locations (Paris, Ghent, Helsinki and Santander) on which the behaviour and performance of the different solutions adopted and implemented was analysed and evaluated.

Contents

List of Figures	S.v
Acronyms	S.vii
S1 Introduction	S.1
S1.1 Motivation and targets	S.3
S1.2 Thesis structure	S.4
S2 Conclusions	S.7
S2.1 Towards Future Internet	S.11
Bibliography	S.15
SA Publications	S.17
SA.1 Book chapters	S.17
SA.2 International journals	S.17
SA.3 International conferences	S.18
SA.4 National conferences	S.20
SA.5 Patent requests	S.20
SA.6 Seminars and invited speeches	S.20
SA.7 Scientific documents	S.22

List of Figures

S1.1 Map of wireless communication technologies	S.3
S1.2 Relation amongst the chapters of the thesis	S.5
S2.1 Future Internet Architecture	S.12

Acronyms

AI	Ambient Intelligence
CPFP	Certified PN Formation Protocol
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
FI	Future Internet
IoK	Internet of Knowledge
IoS	Internet of Services
IoT	Internet of Things
IoU	Internet of Users
IST	Information Society Technologies
MAGNET	My personal Adaptative Global NET
MIP	Mobile IP
OSI	Open Systems Interconnection
PAN	Personal Area Network
PFP	PN Formation Protocol
PKI	Public Key Infrastructure
PN	Personal Network
PNCA	Personal Network Certification Authority
PN-F	Personal Networks Federation
P-PAN	Private Personal Area Network
SCMF	Secure Context Management Framework
SMP	Service Management Platform
UCL	Universal Convergence Layer
WAN	Wide Area Networks
WLAN	Wireless Local Area Networks

ACRONYMS

WPAN	Wireless Personal Area Network

Chapter S1

Introduction

The capability of transformation and adaptation to the environment has marked the evolution of human beings and ambition, as an innate feature, has led it to exceeding limits in the interests of achieving self-imposed goals. Communication, although it is not a distinguishing feature of the human race, has played a central role in its development.

Communication history dates back millions of years; mankind has always looked for ways to share thoughts and actions. The development of language brought with it an evolutionary advantage which mankind took advantage of to pass information on efficiently from generation to generation, to promote knowledge sharing and to coordinate efficiently in order to carry out tasks. The passage of years led to the progressive consolidation of language and then the challenge of defining new more efficient ways of communication arose.

Time and distance have been the serious and obvious limitations of any communication pattern. Not having a symmetrical communication channel where all parties involved can actively participate in information exchange is another. However, mankind has always managed to sort any situation out and that is where technology has come in to make things easier.

Oral language evolved towards writing with the aim of preserving knowledge. Printing, restricted to the most powerful social strata throughout most of ancient history, allowed almost anyone to access culture and from that moment on, evolution underwent a great impulse.

However, it was not until the middle of the 19th century, with Samuel Morse's invention of the first telegraph, that another great communication revolution took place: successful almost instant transmission of a message between two points geographically apart. From that moment on, the advent of the telephone and the radio improved the way information was exchanged.

When the intellectual capability to develop new options was limited, the emergence of the first computers at the end of the first half of last century provoked a new evolutionary impetus, whose acceleration is currently still increasing.

The search for convergence between the computing and communication worlds led, in the sixties, to the envisagement of the Internet as a network which would enable autonomous hubs, distributed and organised in multiple independent networks in different locations, to

share information. A key concept of Internet is that it had not been designed to support a single application but as a generic infrastructure in which new and multiple applications could be deployed. That characteristic has meant that the creation of a small group of researchers can be considered the latest great revolution in the way of sharing knowledge.

Internet was devised as an open architecture network to share resources instead of replicating them. The choice of the access technology was not explicit so it could be selected freely by suppliers and they would make it interact with the rest of the network. This philosophy soon resulted in access to all these resources being enabled through packet networks by satellite, mobile networks, wireless networks and others, in which cable connections were relegated to a second level usually as part of the backbone network.

This tendency was the result of users' demand for more flexible environments which will bring them mobile access capabilities. In this way, resources would be available at any time and place, achieving the so longed-for ubiquity. The way of surmounting the barriers imposed by distance and time had been found.

This need came up in the entrepreneurial world, where access provided by Wide Area Networks (WAN) was initially the major requirement. With the boom of terrestrial mobile and wireless communication technologies at the end of the last millennium, this information access pattern was little by little becoming more popular. In this new environment, requirements changed. The ordinary users bring the service demand closer to them and make the usage of WAN services migrate towards closer services available through Wireless Local Area Networks (WLAN).

The cost of the necessary equipment led to an initial low penetration speed though it was highly desired by many. However, the continuous advance in microelectronic technology integration has not only allowed a significant increase in computing capabilities but has also permitted the integration of a greater number of functionalities in devices, communication access technologies amongst them, while it has lowered manufacturing and sale costs.

As technology has become more accessible and portable, society has demanded the adaptation of services to a more personal context, which has ended up in the development and deployment of a new range of transmission technologies included in the so-called Wireless Personal Area Network (WPAN). These technologies allow the connection of laptops, mobile phones or any other personal device, within a range of up to 10 metres, transparently at high rates and with low power consumption.

The great range of means to access the resources has led to an exponential increase in Internet users throughout the past years and now information access can be considered universal. This was predicted by Bill Gates 20 years ago: 'all the information we need and more is literally at our fingertips and fits in our coat pockets' [1]. However, though information, services, applications and any resource are accessible by means of almost any device, most users do not know how to manage this diversity intelligently and it overwhelms their expectations and what's more, their capabilities.

If a map of the currently available wireless communication technologies is drawn, such as the one shown in figure S1.1, the existence of a great number of them can be seen as the result of the adaptation of each one to a very specific field regarding binary rate, coverage, use, etc. Moreover, interoperability between most of them is not possible.

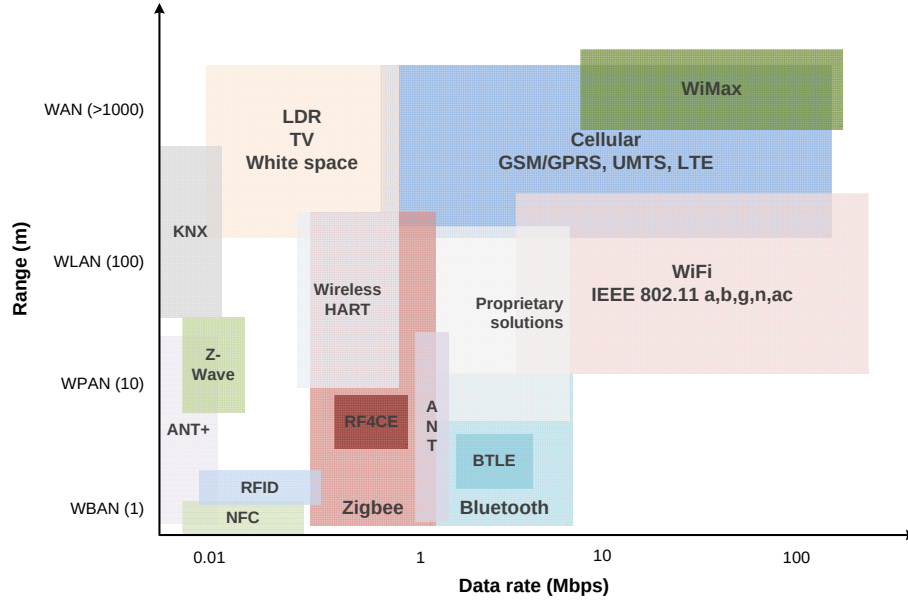


Figure S1.1: Map of wireless communication technologies

The same task could be done for the models and architectures of access devices and the services accessed or provided and the result would be very similar. This in practice means difficulties for the users who have to accept this diversity and acquire enough knowledge of each of them for their use.

Unfortunately, little effort has been made to integrate all these technologies and to give the users the importance they deserve, by offering them a unique use experience, independent and adapted to their needs and preferences. Although it is true that some attempts have been made in various research initiatives, no global solutions have been observed at commercial level. The greatest achievement so far is that each specific company, such as Apple, Google or Microsoft, integrates services, applications and devices of their own ecosystem. However, this is not the desired and expected situation.

S1.1 Motivation and targets

Several shortcomings have been identified within the described framework. Most of them point in one direction, the users. Though the technological evolution has been directed by them, they are also responsible for guiding the instruments, designed and developed by them, in order to carry out the required tasks. Human beings have forgotten that they themselves are both judge and jury and that they should have provided autonomy for the created ecosystem so that it not only acts under their orders but also reacts intelligently to changes in their needs and preferences.

In this sense, as can be inferred from the previous description, the increasing number of user devices, not only those in their closest environment but also those located in their home, office, etc., interact with each other defining a network whose features are no longer generic. This network, which can be named personal, has an obvious approach towards

the user. It should be an intelligent network and more sensitive to context; this will lead the behaviour of the nodes and services which make it up to accommodate its owners' requirements. Therefore, the usage experience of two users with similar equipment could be completely different since the corresponding networks will know them and adapt to them.

The concept of Personal Network (PN) expands that of the traditional Personal Area Network (PAN) as it includes devices and remote services outside the physical reach of the user. It will be the PN itself which will bring the user closer to any of their terminals by enabling a ubiquitous and transparent access through underlying networks. The implications of PN deployment go beyond connectivity provision amongst its nodes and it must ensure interoperability with other networks, such as the Internet, in which there is a great number of added value services available to the user.

Therefore, ubiquity and context are initially two key aspects which give meaning to PNs. Security will be the third and it will make the user trust that their privacy is protected at all times and that data about the services they use or provide others will not be in danger.

Answering questions such as how to achieve a ubiquitous communication experience by means of heterogeneous technologies, which mechanisms to use so as to develop, use and supply services over that network, how to adapt the network response to context and above all how to make the configuration and use of such an ambitious network easier, will make up the developments to be carried out and will provide PN with sound and stable pillars.

S1.2 Thesis structure

The global aim of this study is to define an architecture which provides support to a personal network, as an extension of a PAN, and clusters of them. In order to do so, besides devising different design proposals, it deals with their experimental evaluation so that their viability can be validated.

The methodology used is shown in figure S1.2. Thus, in chapter 2 "Related requirements and initiatives" a set of canonical use cases are analysed and the corresponding requirements are extracted for both, personal networks and their clusters. Then the state-of-the-art is presented, regarding previous initiatives related with some of the concepts mentioned.

As is stressed throughout this document, the user is the main element in any of the solutions. Taking some of the approaches derived from the state-of-the-art study as a reference, firstly architecture for a PN is designed and specified, as the user's own domain, and later it is extended towards the Personal Networks Federation (PN-F) as a domain shared by multiple users.

In chapter 3 "Towards personal networks", three layers are identified in the PN: the abstraction layer at connectivity level, at network level and at service level. These three layers will adapt their behaviour to the user's context. There will be a fourth layer, transversal to all of them, the one which carries out the acquisition, management and provision of context information.

Though basic concepts regarding security are presented in chapter 3, it is in chapter 4

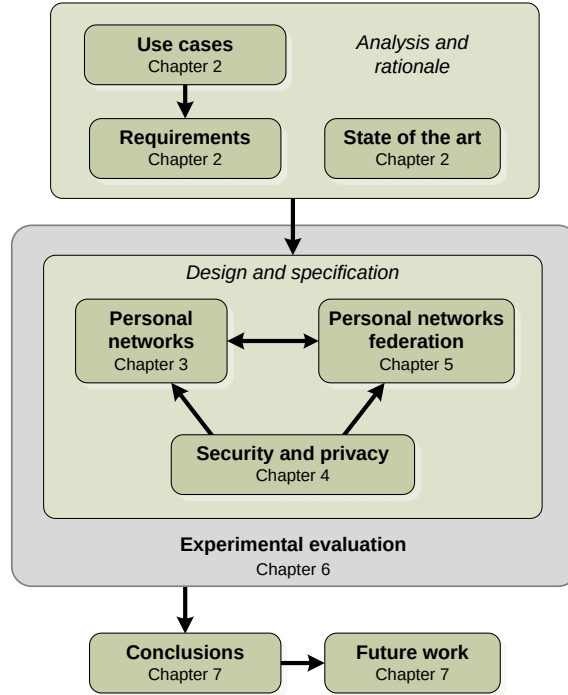


Figure S1.2: Relation amongst the chapters of the thesis

“Security and privacy” where the solutions which make a PN a safe, reliable and private network are presented. In this direction, the procedures which allow a reliable bilateral relation to be established between nodes, ensuring the link with the user, are described. Details are also given about how this relation influences the operations within the abstraction layers mentioned above.

After analysing the PN from all levels as an autonomous entity, the specification section ends with a proposal for a global design of PN-F architecture. Considering a PN-F as an extension to PNs which share resources, and after analysing the requirements, most solutions defined for PNs can be inherited by PN-Fs. Therefore, chapter 5 “Personal networks federation” details the concept of PN-F and its life cycle from its creation to its termination, taking into account the requirements a PN must meet to be part of a PN-F and the mechanisms which ensure confidence and security within the PN-F. In this chapter, a generic architecture is put forward which is particularised according to two approximations: a PN-F considered as an addition supported at network level in which all kinds of resources (connection, services, etc.) are shared or a PN-F considered just at service level.

Chapter 6 “Experimental evaluation” deals with experimental validation of the proposals of this research in the framework of the Information Society Technologies (IST) projects, My personal Adaptive Global NET (MAGNET) and MAGNET Beyond as well as some others carried out in the framework of additional collaborations.

To conclude, chapter 7 “Conclusions” compiles the major contributions and establishes a proposal for investigation lines originating from the research developed in this thesis.

Chapter S2

Conclusions

Digitization and the fast technological advance are opening opportunities unthought-of some years ago, which make society face the most common situations of everyday life very differently. Although aware that technology can help improve society; its global adoption by citizens has surpassed any forecast. It is not difficult to encounter someone who is carrying multiple devices, such as a laptop, mobile phone, tablet, smart watch, heart rate monitor or other sensors, amongst others.

All this diverse equipment is envisaged to be at the user's service, as it is supposed that it allows a user-friendly information access at any time and place. However, the most common situation is the opposite and the user has ended up adapting to the devices, facing the tedious and complex configuration processes and overcoming their ignorance and the barriers they impose.

Thus, of the five attributes proposed by Everett M. Rogers [2], which determine 'the adoption or rejection of an innovation, including the technological ones: relative advantage, compatibility, complexity, trialability, and observability', there are still several to be resolved in the environment presented.

It is obvious that the evolution of the relationship between users and their devices still presents a lot of room for improvement before full device servitude is achieved. In this respect, from a series of usage cases providing an example of what the researcher understands a personal network should be, a series of requirements every personal network must meet were extracted; these requirements drove the development of the study.

This thesis presented the Personal Network (PN) as a novel network model, which expands the paradigms of PAN and Ambient Intelligence (AI), and aims to fill the shortcomings current networks have regarding adaptation to users. Hence, the PN has emerged as a cluster of all the user's devices, regardless of their features and location, which enables a secure heterogeneous communication amongst them with the aim of satisfying the user's needs. All PN nodes or personal nodes share a reliable relationship certified by the user.

The concept of PN focuses on simplifying and fostering the coexistence of a user with their devices and services. This search for simplicity has led to a reduction in complexity and restrictions in traditional network architecture. For this reason, a new architecture model based on abstraction layers is devised. Three main levels are defined (as opposed

to the seven of the Open Systems Interconnection (OSI) model), linked to connectivity at link level, to interaction at network level and to service management; these levels are provided with freedom to exchange information amongst themselves. There is a fourth level, associated with user context, their devices and the network they make up, which has a layout transverse to the other three and enables flow amongst them.

On tackling the study of the link and network levels, it was found that heterogeneity in the kinds of devices is extensible to the communication technologies available within them. Nowadays, it is not possible to imagine a device with a single communication interface. To face the challenge of this diversity, this study contributed to the definition and further development of a Universal Convergence Layer (UCL) which hides all underlying complexity regarding communication technologies at network level. Its modular design has enabled the extension of its functionalities including autonomous management of communication interfaces, establishment of reliable direct channels amongst nodes and acquisition and intelligent use of statistics from the communication channel as part of the context, which were described and evaluated. The experimental results obtained with the implementation developed demonstrate that the UCL goes a step beyond the existing solutions in the field of cross-layer optimisation, opening the way towards the application of new cognitive communication strategies.

After solving the problems heterogeneity causes in communications amongst nodes at link level, at network level, first the way user nodes gather together and communicate with each other was defined and then the way nodes in different clusters establish end-to-end connexions was explained.

Trying to maintain the independence of data flow generated amongst communication nodes and non-personal nodes, PN architecture was based on a virtual overlay network with its own private addressing, whose specification is described in depth throughout this report. All nodes of a PN, simply by belonging to the same user, share a bilateral relationship which supports the trust amongst them and constitutes the unifying element of the network. This is why clusters, as they were defined in a PN, are not only additions of nearby nodes capable of communicating amongst each other but, as an innovation, the requirement is added of the existence of that mutual trust relationship, a criterion which was used to determine the optimum route amongst nodes. The UCL, in collaboration with a neighbour discovery module, allows the identification of close nodes and the definition of the cluster limits. Given the importance of the user in a PN, the closest nodes to them make up a special cluster which is denominated Private Personal Area Network (P-PAN).

The clusters of a PN are generated either spontaneously or in a way predefined by the user and they do not depend on the infrastructure. For this reason, it was decided to use ad-hoc router solutions for the links between its nodes. On the other hand, communications amongst nodes from different clusters rely on the interconnection infrastructure, establishing direct tunnels which encapsulate personal traffic. The network solution presented also includes support for mobility, an indispensable requirement to meet when it comes to providing ubiquitous communication. Adapting the solution specified, already developed in the context of the MAGNET project, this thesis included the experimental validation of mobility by using a standard solution such as Mobile IP (MIP)v6 deployed in user devices such as smart mobile phones.

Although the possibility of using the completely distributed network architecture was described, a hybrid solution was finally decided on, with an intermediary entity, the PN Agent, which frees the user nodes from functionalities during the remote communication channel establishment and, as was seen later, also facilitates the maintenance of the confidence relationships within a PN and the interaction amongst PNs.

On top of the overlay network defined, nodes will exchange information associated with services. This thesis proposes a Service Management Platform (SMP), covering the whole service lifecycle, divided in four major functional domains: creation, publication and discovery, implementation and provision and user platform. It was observed that the tasks carried out in each of them were influenced by the component-oriented approach in defining a service and the inherent heterogeneity of a PN.

As for the PN architecture, the aim of context awareness, one of the major requirements proposed at the beginning of this thesis, was addressed. This was achieved by the transverse layer which unifies context management within the PN. The Secure Context Management Framework (SCMF), with functional architecture similar to the SMP, provides the functionalities of discovery, maintenance, processing and distribution of context information. Not all functionalities can run within any personal node and that is the reason why some tasks are delegated to more powerful nodes. As part of the validation tasks of the SCMF, a procedure for the discovery, selection and maintenance of the node which can best take charge of the functions required by the SCMF was developed and validated both by simulation and in a real environment.

Within a PN, context information not only includes the user's environment and their devices but also their preferences. The SCMF offers interfaces which allow the user or any other component of the PN to provide information associated with context, described according to an ontology, which will be internally processed to give it added value. In this respect, the development carried out to validate the UCL included some interfaces compatible with those required by the SCMF along with the adaptation of the statistics obtained to the ontology defined for the PN. The SCMF also includes output interfaces to obtain context information.

Up to this point, almost all requirements identified (ubiquitous communications, service management, context awareness and ease of use) were given an answer except those related to security. Although in the descriptions of the PN architecture certain security mechanisms were mentioned, all security aspects were brought together in a single section to ease comprehension.

Based on the studies carried out in [3–5], the PN security architecture was defined. A node acquires the status of personal by belonging to a user. However, to establish a reliable communication with others, it must be able to share its status. Initially in this thesis, the use of the PN Formation Protocol (PFP) was proposed; through it and with the participation of the user, whichever two personal nodes recognise themselves and establish a bilateral trust relationship represented by a shared key. However, the first approximation carried out showed potential deficiencies when scaled, making the PN less attractive. For this reason, its definition was updated and its distributed approach was changed to one based on a Public Key Infrastructure (PKI) adapted to the personal environment. The result of the Certified PN Formation Protocol (CPFP) is also the recognition of the personal

condition between two nodes, but it improves PFP because it facilitates scalability. In this respect, this thesis adds a distributed strategy for management of Certificate Revocation Lists (CRLs) which attempts to eliminate security risks derived from the loss of personal nodes. Additionally, to strengthen the PN security layer, a hierarchical methodology is explained for diversification of the bilateral key, depending on the abstraction layer to be ensured. This scheme was included in the implementation of the UCL and it is the basis of personal node identification. In this way, the viability of the strategy and simplicity for the user in securing communications amongst their equipment was demonstrated.

Once the PN architecture was designed, specified and validated, the next step was to define a solution which allowed several PNs to operate collaboratively. If users interact with one another, their networks must work the same way. Hence the concept of PN-F emerges as the environment where users share the available resources of their PN safely and in an orderly way.

The establishment of a PN-F requires more complex procedures than those for a PN because they must ensure the fulfilment of each PN-F participant's will. In this respect, a PN-F full life cycle was developed. The description starts by defining the PN-F profile, which details the aims and conditions to be met in order to participate in the PN-F, and the user's profile, which lists the elements to be shared, with details of how, with whom and under what circumstances. The profiles will guide the process of formation and use of the PN-F. Both profiles must have common conditions so that the potential member becomes an active part of the PN-F. After describing the operation of the PN-F, the specification of a generic architecture is defined. This specification will later be particularised according to two approaches. The first one considers the PN-F as a natural extension of the PN and therefore it defines it as a virtual overlay network. In this kind of PN-F, users can share any resources, connexion or service capability. The other approach allows the formation of a PN-F taking into account only the services. Both cases offer solutions to give support to PN-Fs, either spontaneously generated on an ad-hoc basis or generated from a pre-established agreement, providing an answer to the usage needs observed.

Indeed, security and terms of use validation in both approaches were stressed; for this purpose, the specific entities which must be added to PNs were provided. Moreover, a new entity to certify PN identity and profiles was defined by extending the personal PKI hierarchy. In this respect and included in the experimental validation carried out, a methodology was proposed based on smart cards as secure elements; this ensures the start-up processes of a Personal Network Certification Authority (PNCA) and facilitates the establishment of secure and reliable relationships amongst PNs.

Although it has already been mentioned in previous descriptions, it must be stressed that the studies carried out were not limited to theoretical analysis, but the solutions presented were also validated in real environments. Some of the most relevant were included in this thesis, although throughout all the research projects in which the author participated during the years leading to this thesis, namely MAGNET, MAGNET Beyond or mIO!, the author actively collaborated in the integration and validation of almost all of the components described.

This thesis clearly demonstrated a strategy for tackling personal networks and the collaboration amongst them. Although most of the protocols and mechanisms used are being

widely used by the scientific community, it can still be considered that some of the proposals are far from technological reality. However, the adaptation of the solutions proposed to more usual environments closer to the user, without abandoning the philosophical ideas behind the PN and the PN-F, would allow a more direct application as was shown. In this respect, and as an example, the latest generation mobiles already support certain schemes to manage the heterogeneity of communications and multi-hop communications are successfully being used to enable the connexion with and amongst sensor devices distributed in environments which are difficult to access.

The standardisation work being developed in the field of the ECMA TC32 [6] and European Telecommunications Standards Institute (ETSI) [7] is expected to make PN and PN-F known to the industry so that their gradual integration can start. With the advent of Internet of Things (IoT), the transfer of some of the ideas considered in a PN has begun. On the one hand, the sensors themselves configure, discover and interact autonomously by using multi-hop routing protocols and keeping communications secure both at link and end-to-end levels. On the other hand, the environment data acquisition carried out by the sensors allows the inference of new information patterns which can provide added value services.

Both PN and PN-F were two innovative concepts originated a few years before the boom of social networks such as Facebook or Twitter. Social networks, as they are currently known, allow users to share personal multimedia resources, their location or their thoughts at a given time. However, they do not consider the interaction between the devices they have. In this respect, the words of one of Twitter creators, Evan Henshaw-Plath, are revealing; during the 4th Congress of Bright Minds which took place in Madrid, he set out, as futuristic concepts, that devices should offer or generate information ‘according to the circumstances (where we are, with whom, our vital signs, etc.)’ or the approach to ‘a network which connects people who happen to meet in the same hall without them having to do anything’, both aspects already considered within a PN and a PN-F.

S2.1 Towards Future Internet

The concepts of PN and PN-F were approached and analysed from multiple perspectives throughout this thesis. However, as open architecture, the possibility of introducing alternatives which permit us to go beyond the results obtained here was left open. As was discussed, the success of the PN and the PN-F will be given by their acceptance and adoption by the industry.

Therefore, it is considered that the natural projection of the investigation and development tasks related to PN and PN-F is an extension of these concepts towards the Future Internet (FI). The FI is made up of four pillars based on a new network infrastructure as its basis. These pillars are: IoT, Internet of Services (IoS), Internet of Knowledge (IoK) and Internet of Users (IoU) whose correspondence is shown in figure S2.1. The coexistence and convergence of all of them will provide the user with a safe, reliable and sound environment which allows access to the network and its information to be open, dynamic and decentralised, while adapting to the users’ needs and their context. Since their conception, the studies on PN and PN-F have followed a line directed, without a doubt, in that direction.

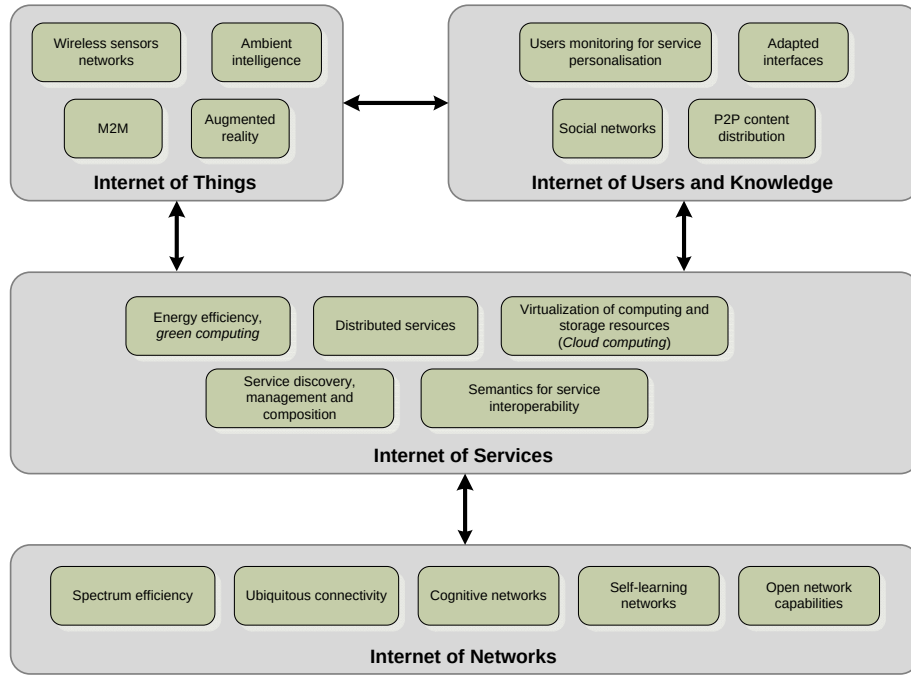


Figure S2.1: Future Internet Architecture

The conclusions showed how IoT deployments include ideas proposed in this thesis, mainly those directed to the establishment of secure connectivity amongst nodes. In these deployments, each sensor node captures global information on the environment which is jointly analysed with that of other sensors to infer added value information. The data provided is linked to a wider domain than that of a single sensor.

Thus, the challenges the IoT faces include, amongst others, the investigation of new methods to transmit data dynamically, either synchronously or asynchronously, on very heterogeneous environments and its further processing. These solutions must be scaled up properly to remain balanced and to avoid past mistakes which led to saturation of networks without having fulfilled the expectations and technological challenges proposed.

The IoT model led, amongst others, to the smart city paradigm used within the IST project Smart Santander Project [8]; this project proposes a unique experimental platform in the world to provide support to the services of a smart city. Its aim is to design, deploy and validate a platform made up of 20,000 devices (sensors, collectors, actuators, cameras, mobile terminals, etc.) creating a virtual space where objects communicate with each other and transmit useful information with the aim of improving citizens' quality of life.

Generally speaking, the information collected by the set of IoT devices enables the development of numerous services which will be offered, used or adapted by a wide range of suppliers, consumers or service aggregators. This new way of offering functionalities is booming in the IoS. One of the major challenges the IoS faces is the integration of different layers of services, from infrastructure services to specific services with a user interface. The solution lies in the intelligent organization of services and their customisation to their execution context as well as in the use of cloud computing. Projects such as mIO! tried to

apply these approximations from the entrepreneurial and user point of view. The results obtained demonstrate the viability of the approach but they also report that the technology required is not available yet, at least for the end user. The numerous obstacles to surmount leave open ways to explore new approaches.

The implementation of the two previous models has certain independence from the IoU for the time being. The IoU is closely linked to the IoK, as both try to apply customisation to context and to users' preferences and needs as a way to provide a better usage experience; this is the reason why they were shown together in figure S2.1. In order to achieve this target, it is necessary to know more about the user (their habits, tastes, etc.) and those they socialise with. The value this information has is directly reflected in the capitalisation of companies related to social networks; these companies, although their business model is not at all clear, are the first ones to have started the capture of that data. However, though users' behaviour can be anticipated and given that technology is closer and closer, users also demand more power and self-management.

It should be mentioned that some projects are emerging, proposing the necessary steps to make the user the centre of the ecosystem. This is the case of the IST project SOCIOTAL [9] whose aim is to devise techniques which allow the adoption of the IoT, eliminating users' fears regarding aspects related to privacy and safety.

Overcoming all the barriers described means a huge challenge to make the FI happen. The PN and the PN-F have presented a possible approach. Now it is time to offer new alternatives for the benefit of consumers and providers.

Bibliography

- [1] B. Gates, “Information At Your Fingertips, Keynote Speech”, in *COMDEX*, ser. MobiCom '04, Alladin Hotel, Las Vegas, Nevada, USA, Nov. 1994.
- [2] E. M. Rogers, *Diffusion of Innovations, 5th Edition*, 5th. Free Press, Aug. 16, 2003, ISBN: 0743222091.
- [3] I. Gkanas, V. Kaldanis, A. Markopoulos, *et al.*, “State of the art and Functional Specification of Network-Level Security Architecture”, MAGNET (My personal Adaptive Global NET), Deliverable 4.3.1, Sep. 2004.
- [4] S. Mirzdeh, C. Politis, K. Nyberg, *et al.*, “Final version of the Network-Level Security Architecture Specification”, MAGNET (My personal Adaptive Global NET), Deliverable 4.3.2, Feb. 2005.
- [5] J. Jaen Pallares, H. Affi, M. Argyropoulos, *et al.*, “Selections and Implementation of protocols and solutions in the view of PN-Platform”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 4.1.2, Feb. 2007.
- [6] ECMA International TC32, “Personal Networks - Overview and Standarization Needs”, ECMA International, Tech. Rep., Dec. 2010. URL: <http://www.ecma-international.org/memento/TC32-PNF-M.htm>.
- [7] “eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth”, Tech. Rep. 102 431 v1.1.1, Feb. 2009.
- [8] SmartSantander, *FP7-IST-257992*, 2010. URL: <http://www.smartsantander.eu> (last visit on 2014).
- [9] SOCIOTAL, *Creating a socially aware citizen-centric Internet of Things, FP7-IST-609112*, 2013. URL: <http://sociotal.eu/> (last visit on 2014).

Appendix SA

Publications

Finally, it is necessary to mention that the contributions presented here have originated several publications.

SA.1 Book chapters

- E. Kovacs, L. Sanchez, **J. Lanza**, J. Hoebeke, M. G. Genet, M. Bauer, R. L. Olsen, M. Ghader, H. Thuvesson, and L. Muñoz, “PN networking”, in *My Personal Adaptive Global NET (MAGNET)*, 1st, ser. Signals and Communication Technology. Springer Publishing Company, Inc., 2010, ch. 3, pp. 75–134, ISBN: 9789048134366, 978-90-481-3437-3.
- J. Zidbeck, L. Sanchez, K. Ahola, M. Alutoin, M. Bauer, S. Bessler, M. G. Genet, J. Hoebeke, **J. Lanza**, I. Moerman, R. L. Olsen, J. J. Pallares, and J. Zeiss, “PN Platforms”, in *My Personal Adaptive Global NET (MAGNET)*, 1st, ser. Signals and Communication Technology. Springer Publishing Company, Inc., 2010, ch. 7, pp. 337–407, ISBN: 9789048134366, 978-90-481-3437-3.

SA.2 International journals

- L. Sánchez, I. Elicegui, J. Cuesta, L. Muñoz, and **J. Lanza**, “Integration of Utilities Infrastructures in a Future Internet Enabled Smart City Framework”, *Sensors*, vol. 13, no. 11, pp. 14 438–14 465, 2013, ISSN: 1424-8220.
- L. Sánchez, **J. Lanza**, L. Muñoz, and K. A. M. Alutoin, “Securing the Communication in Private Heterogeneous Mobile Ad hoc Networks”, *Wireless Personal Communications*, vol. 52, no. 2, pp. 393–409, 2010, ISSN: 0929-6212.
- L. Sánchez, **J. Lanza**, and L. Muñoz, “Optimisation of dynamic interface selection mechanisms on multi-radio devices in ad hoc networks”, *Electronics Letters*, vol. 45, no. 11, pp. 558–559, May 2009, ISSN: 0013-5194.

- L. Sánchez, **J. Lanza**, and L. Muñoz, “Extending Private Personal Area Networks to Personal Network Federations in heterogeneous ad-hoc scenarios”, *Special issue on Personal Networks of Teletronic journal*, vol. 103, no. 1–2007, pp. 34–44, Feb. 2007, ISSN: 0085-7130.
- D. M. Kyriazanos, M. Argyropoulos, L. Sánchez, **J. Lanza**, M. Alutoin, J. Hoebeke, and C. Z. Patrikakis, “Overview of a Personal Network Prototype”, *IEC Annual Review of Communications*, vol. 59, 2006.
- L. Sánchez, **J. Lanza**, and L. Muñoz, “Experimental Assessment of a Cross-Layer Solution for TCP/IP Traffic Optimization on Heterogeneous Personal Networking Environments”, *Lecture Notes in Computer Science*, vol. 4217, pp. 284–296, Sep. 2006, ISSN: 0302-9743.

SA.3 International conferences

- J. Rico, B. Cendon, **J. Lanza**, and J. Valiño, “Bringing IoT to Hospital Logistics Systems Demonstrating the concept”, in *Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE*, Apr. 2012, pp. 196–201.
- L. Sanchez, **J. Lanza**, and L. Muñoz, “Energy Efficiency of Dynamic Interface Selection Mechanisms in Wireless Ad-Hoc Networks”, English, in *Mobile Networks and Management*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, K. Pentikousis, R. Agüero, M. García-Arranz, and S. Papavassiliou, Eds., vol. 68, Springer Berlin Heidelberg, 2011, pp. 188–197, ISBN: 978-3-642-21443-1.
- **J. Lanza**, L. Sánchez, and L. Muñoz, “Experimental Comparison of Two Solutions for Securing Heterogeneous Ad-Hoc Network Communications”, in *11th International Symposium on Wireless Personal Multimedia Communications*, Lapland, Finland, Sep. 2008.
- L. Sánchez, **J. Lanza**, J. Hoebeke, I. Moerman, M. Alutoin, K. Ahola, J. J. Pallares, M. G. Genet, M. Bauer, and J. Zeiss, “Assessing Personal Networks on a pan-European Testbed”, in *ICT Mobile and Wireless Communications Summit 2008*, Stockholm, Sweden, 2008.
- R. Olsen, M. Bauer, L. Sanchez, and **J. Lanza**, “Self Organisation of Context Agents in Personal Networks and Federations”, in *10th International Symposium on Wireless Personal Multimedia Communications*, Jaipur, India, Jun. 2007.
- L. Sánchez, **J. Lanza**, and L. Muñoz, “Federating Personal Networks over Heterogeneous Ad hoc Scenarios”, in *12th IFIP International Conference on Personal Wireless Communications*, S. I. Series, Ed., vol. 245, Prague, Czech Republic, Sep. 2007, pp. 38–53.

- L. Sánchez, **J. Lanza**, J. Rico, and L. Muñoz, “Implementation of a Vertical Handover Solution for Coexisting Ad-hoc Multihop and Infrastructure Access Networks based on IEEE 802.11”, in *7th International Workshop on Applications and Services in Wireless Networks*, Santander, Spain, May 2007, pp. 15–21, ISBN: 978-84-690-5727-8.
- M. Bauer, R. L. Olsen, M. Jacobsson, L. Sánchez, **J. Lanza**, M. Imine, and N. Prasad, “Context Management Framework for MAGNET Beyond”, in *15th IST Mobile & Wireless Summit Communications Summit*, Mykonos, Greece, Jun. 2006.
- M. Ghader, R. L. O. Olsen, V. Prasad, M. Jacobsson, L. Sánchez, **J. Lanza**, W. Louati, M. Girod Genet, D. Zeghlache, and R. Tafazolli, “Service Discovery in Personal Networks: design, implementation and analysis”, in *15th IST Mobile & Wireless Summit Communications Summit*, Mykonos, Greece, Jun. 2006.
- J. Hoebeke, G. Holderbeke, I. Moerman, W. Louati, W. Louati, M. Girod Genet, D. Zeghlache, L. Sánchez, **J. Lanza**, M. Alutoin, K. Ahola, S. Lehtonen, and J. Jaen Pallares, “Personal Networks: From concept to a demonstrator”, in *15th IST Mobile & Wireless Summit Communications Summit*, Mykonos, Greece, Jun. 2006.
- **J. Lanza**, L. Sánchez, and L. Muñoz, “Cluster Head Selection and Maintenance over Heterogeneous Mobile Wireless Personal Area Networks. an experimental approach”, in *9th International Symposium on Wireless Personal Multimedia Communications*, San Diego (CA), USA, Sep. 2006.
- **J. Lanza**, L. Sánchez, and L. Muñoz, “Performance Evaluation of a Cross-layer based Wireless Interface Dynamic Selection on WPAN/WLAN Heterogeneous Environments: An Experimental Approach”, in *6th International Workshop on Applications and Services in Wireless Networks*, Berlin, Germany, May 2006, pp. 139–146, ISBN: 3-8167-7111-4.
- L. Sánchez, **J. Lanza**, M. Bauer, R. L. Olsen, and M. Girod Genet, “A Generic Context Management Framework for Personal Networking Environments”, in *The Third Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, San Jose (CA), USA, Jul. 2006, pp. 1–8, ISBN: 0-7803-9792-4.
- M. Alutoin, K. Ahola, S. Lehtonen, L. Sánchez, **J. Lanza**, J. Hoebeke, G. Holderbeke, I. Moerman, M. G. Genet, and W. Louati, “Self-organisation and mobility in Personal Networks”, in *8th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, Sep. 2005, pp. 318–322, ISBN: 87-90834-82-8.
- M. Alutoin, S. Lehtonen, J. Hoebeke, G. Holderbeke, I. Moerman, L. Sánchez, **J. Lanza**, D. Zeghlache, and W. Louati, “Towards Self-organising Personal Networks”, in *1st ACM Workshop on Dynamic Interconnection of Networks*, Collogne, Germany, Sep. 2005, pp. 12–16, ISBN: 1-59593-144-9.
- L. Sánchez, **J. Lanza**, and L. Muñoz, “Self-Configuring Private Personal Area Networks: The first stage towards Personal Networking”, in *8th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, Sep. 2005, pp. 1983–1987, ISBN: 87-90834-82-8.

- L. Sánchez, **J. Lanza**, L. Muñoz, and J. Perez, “Enabling Secure Communications over Heterogeneous Air Interfaces: Building Private Personal Area Networks”, in *8th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, Sep. 2005, pp. 1963–1967, ISBN: 87-90834-82-8.

SA.4 National conferences

- L. Sánchez, **J. Lanza**, and L. Muñoz, “Eficiencia Energética de un Mecanismo de Selección Dinámica de Interfaces en Redes Ad-hoc Inalámbricas”, in *X Jornadas de Ingeniería Telemática*, Santander, Spain, Sep. 2011, pp. 245–250, ISBN: 978-84-694-5948-5.
- L. Sánchez, **J. Lanza**, J. Choque, L. Muñoz, and D. González, “Arquitectura de una Entidad Middleware para la Gestión Cognitiva de las Comunicaciones en Terminales Multiradio”, in *IX Jornadas de Ingeniería Telemática*, Valladolid, Spain, Sep. 2010, ISBN: 978-84-693-5398-1.
- L. Sánchez, **J. Lanza**, L. Muñoz, and J. Rico, “Redes Personales: la implementación del concepto”, in *XVII Jornadas TELECOM I+D*, Valencia, Spain, Feb. 2007.
- R. Agüero, L. Muñoz, J. Choque, L. Sánchez, and **J. Lanza**, “Estudio experimental de los protocolos IP en redes inalámbricas multi-salto basadas en el protocolo DSR”, in *V Jornadas de Ingeniería Telemática*, Vigo, Spain, Sep. 2005, pp. 217–224, ISBN: 84-8408-346-2.
- **J. Lanza**, R. Beivide, and R. Menendez, “Plataformas distribuidas para calculo paralelo”, in *XI Jornadas de Paralelismo*, Granada, Spain, Sep. 2000, ISBN: 87-90834-82-8.

SA.5 Patent requests

- J. Jaen-Pallares, L. Sánchez, **J. Lanza**, and L. Muñoz, *Method for distributing a Certificate Revocation List in a network*, Solicitud de patente 08167197.6, Oct. 2008.
- L. Muñoz, **J. Lanza**, O. Blanco, J. A. Torrero, L. Rodriguez, O. Blanco, P. Real, and M. Gorricho, *Método de autenticación de usuarios para acceso a aplicaciones informáticas y firma de documentos electrónicos a través del teléfono móvil*, Solicitud de patente P200302370, Oct. 2003.

SA.6 Seminars and invited speeches

- **J. Lanza**, “Host Card Emulation: Moving smartcards to the cloud”, in *II Internacional Congress University Smart Card*, Murcia, Spain, Apr. 2014.
- **J. Lanza**, “Public transport and University Smart Card”, in *II Internacional Congress University Smart Card*, Murcia, Spain, Apr. 2014.
- **J. Lanza**, “Smart Cards Fundamentals and Beyond”, ERASMUS IP 2014, University of Cantabria, Santander, Spain, May 2014.

- **J. Lanza**, “University of Cantabria - Use Case Beyond just a Campus Card”, in *12th European Campus Card Conference*, Santander, Spain, May 2014.
- **J. Lanza**, “New Challenges on Campus Smart Cards”, in *11th European Campus Card Conference*, Porto, Portugal, May 2013.
- **J. Lanza**, “TUI santander: a University Smartcard Standard”, in *I Internacional Congress University Smart Card*, Murcia, Spain, May 2013.
- **J. Lanza**, “Las Smart Cities y el Comercio”, in *Jornada Sociedad, Ciudad y Comercio*, Burgos, Spain, Nov. 2012.
- **J. Lanza**, “The Smart Card in the Smart University”, in *10th European Campus Card Conference*, Lund, Sweden, May 2012.
- **J. Lanza**, “Santander Universities Smart Card: The Prepaid Card”, in *8th European Campus Card Conference*, Waterford, Ireland, May 2010.
- **J. Lanza** and V. Prior, “Identificación Digital. Experiencia en las universidades”, in *El gobierno electrónico de la universidad*, Universidad Internacional de Andalucía, Tetuán, Marrocco, Jul. 2006.
- L. Muñoz, L. Sánchez, **J. Lanza**, M. Alutoin, S. Lehtonen, D. Zeghlache, M. Girot Genet, W. Louati, I. Moerman, J. Hoebeke, G. Holderbeke, M. Ghader, and M. Jacobsson, “A proposal for self-organizing Personal Networks”, in *WWRF meeting 15*, Paris, France, Dec. 2005.
- **J. Lanza**, “Smart Cards and Digital Signature”, in *2nd European Campus Card Conference*, London, Great Britain, Jun. 2004.
- **J. Lanza**, “Seguridad en tarjetas inteligentes”, in *Seguridad en Redes Informáticas y de Telecomunicaciones*, Cursos de Verano de la Universidad de Cantabria, Laredo, Spain, Aug. 2003.
- **J. Lanza**, “Tarjetas Inteligentes. Un soporte seguro”, in *NeoCom*, Asociación de Estudiantes de Telecomunicaciones de la Universidad de Zaragoza, Zaragoza, Spain, Dec. 2003, ISBN: 84-7653-824-3.
- **J. Lanza** and L. Muñoz, “The WAL: A performance enhancing proxy for heterogeneous access”, in *Workshop on Internet Usage over 2.5G and 3G*, Barcelona, Spain, Mar. 2003, pp. 134–143, ISBN: 84-7653-824-3.
- **J. Lanza** and O. Blanco, “Java Card Programming: The practical experience of the University of Cantabria”, in *1st European Campus Card Conference*, Waterford, Ireland, Jun. 2002.

SA.7 Scientific documents

- All WP2 Partners, “Second federation architecture”, Federation for FIRE, Deliverable 2.4, Mar. 2014.
- M. Sawyer, G. Francis, I. Panourgias, P. Sotres, **J. Lanza**, D. Margery, J. Lefeuvre, and F. Schreiner, “Report on first cycle developments of the services and applications community”, Federation for FIRE, Deliverable 4.3, Mar. 2014.
- F. Lobillo, M. Sawyer, G. Francis, **J. Lanza**, P. Sotres, B. Bochow, M. Smirnov, B. Vermeulen, and D. Margery, “Second input from the Services and Applications community to the architecture”, Federation for FIRE, Deliverable 4.2, Nov. 2013.
- O. Mehani, G. Jourjon, Y. Al-Hazmi, W. Vandenberghe, D. Stavropoulos, **J. Lanza**, K. Choumas, L. Sanchez, and P. Sotres, “Detailed specifications for first cycle ready”, Federation for FIRE, Deliverable 6.1, Mar. 2013.
- J. V. Ooteghem, B. Naudts, W. Vandenberghe, B. Vermeulen, S. Bouckaert, S. Taylor, P. Grace, F. Lobillo, J. Martrat, L. Muñoz, **J. Lanza**, P. Sotres, and M. Sawyer, “First Sustainability Plan”, Federation for FIRE, Deliverable 2.3, Jul. 2013.
- F. Lobillo, M. Sawyer, S. Taylor, K. Kavoussanakis, **J. Lanza**, L. Muñoz, P. Sortres, and D. Margery, “First input from community to architecture”, Federation for FIRE, Deliverable 4.1, Nov. 2012.
- B. Vermeulen, W. Vandenberghe, T. Leonard, T. Friedman, F. Schreiner, K. Kavoussanakis, M. Ott, F. L. Vilela, P. Sotres, and **J. Lanza**, “First federation architecture”, Federation for FIRE, Deliverable 2.1, Dec. 2012.
- AT4 Wireless, Caja Navarra, Telefónica I+D, Telvent, Universidad de Málaga, **Universidad de Cantabria**, and WorldNet21, “Análisis de la seguridad y confidencialidad para aplicaciones críticas”, Proyecto CENIT mIO!, Entregable 5.3.3, 2011.
- AT4 wireless, Inabensa, **Universidad de Cantabria**, and Universidad de Vigo, “Soporte de publicación de interfaces de acceso proporcionadas por la infraestructura o por dispositivos de terceros”, Proyecto CENIT mIO!, Entregable 6.5.6, Dec. 2011.
- AT4 wireless, Inabensa, **Universidad de Cantabria**, Universidad Politécnica de Cartagena, and Centro Tecnológico de Telecomunicaciones de Cataluña, “Soporte de trasposos de tecnologías de comunicación en redes 3G y WLAN. Aspectos de admisión y QoS”, Proyecto CENIT mIO!, Entregable 6.5.6, Dec. 2011.
- Cemitec, Telefónica I+D, Telvent, Treelogic, and **Universidad de Cantabria**, “Activos Experimentales”, Proyecto CENIT mIO!, Entregable 4.7.2, Dec. 2011.
- Inabensa, AT4 Wireless, Universidad de Vigo, and **Universidad de Cantabria**, “Especificación, diseño y selección de los sistemas de comunicación con las interfaces de acceso en función del servicio”, Proyecto CENIT mIO!, Entregable 6.1.3, 2011.

- Inabensa, AT4 Wireless, Universidad de Vigo, and **Universidad de Cantabria**, “Estudio y definición de modelos de seguridad para las comunicaciones con los interfaces que proporcionan los dispositivos de terceros”, Proyecto CENIT mIO!, Entregable 6.1.4, 2011.
- Inabensa, AT4 wireless, Worldnet21, Centro Tecnológico de Telecomunicaciones de Cataluña, Universidad de Málaga, **Universidad de Cantabria**, and Universidad de Castilla La Mancha, “Técnicas de cognitive radio, que permiten la compartición del espectro entre distintas comunicaciones inalámbricas ”, Proyecto CENIT mIO!, Entregable 6.2.7, 2011.
- Telefónica I+D and **Universidad de Cantabria**, “Configurador de parámetros de red empleando tecnologías NFC y tarjeta inteligente”, Proyecto CENIT mIO!, Entregable - Activo Experimental 4.5.3_AE_5, Jan. 2011.
- Telefónica I+D and **Universidad de Cantabria**, “Estudio de casos de uso en entornos de distribución”, Proyecto CENIT mIO!, Entregable 4.5.3, Dec. 2011.
- Telefónica I+D and **Universidad de Cantabria**, “Estudio tecnológico para el modelado y desarrollo de servicios de retail”, Proyecto CENIT mIO!, Entregable 4.5.2, Jun. 2011.
- Telefónica I+D, **Universidad de Cantabria**, Telvent, Treelogic, Cemitec, and World-Net 21, “Metodologías de desarrollo de servicios en entornos inteligentes”, Proyecto CENIT mIO!, Entregable 4.6.2, Dec. 2011.
- Telvent, ECSC, Robotiker, Telefónica I+D, Treelogic, and **Universidad de Cantabria**, “Mecanismos para la orquestación de servicios”, Proyecto CENIT mIO!, Entregable 4.7.1, Jan. 2011.
- Worldnet21, Telvent, Telefónica I+D, **Universidad de Cantabria**, AT4 wireless, Universidad de Málaga, Universidad de Castilla La Mancha, Universidad Rey Juan Carlos, Inabensa, and Universidad de Vigo, “Análisis de topologías, arquitecturas y tecnologías de interconexión en entornos inteligentes con gran número de elementos distribuidos”, Proyecto CENIT mIO!, Entregable 5.3.5, Dec. 2011.
- AT4 Wireless, Inabensa, Robotiker, Telefónica I+D, Telvent, Universidad Cantabria, Universidad de Vigo, Universidad Rey Juan Carlos, and Worldnet21, “Definición de técnicas de nivel físico para el posicionamiento de alta precisión en exteriores e interiores”, Proyecto CENIT mIO!, Entregable 5.2.1, Feb. 2010.
- AT4 Wireless, Inabensa, Robotiker, Telefónica I+D, Telvent, Universidad de Vigo, Universidad Rey Juan Carlos, **Universidad de Cantabria**, and Worldnet21, “Modelos y métodos de integración de dispositivos de distinta naturaleza”, Proyecto CENIT mIO!, Entregable 5.2.2, Feb. 2010.
- AT4 wireless, Inabensa, Robotiker, Telefónica I+D, Telvent, **Universidad de Cantabria**, Universidad de Vigo, Universidad Rey Juan Carlos, and WorldNet21, “Especificación de estrategias para el roaming de servicios entre diferentes contextos y redes”, Proyecto CENIT mIO!, Entregable 5.2.4, Feb. 2010.

- AT4 wireless, Inabensa, and **Universidad de Cantabria**, “Análisis de los requisitos de gestión en función de los servicios en movilidad”, Proyecto CENIT mIO!, Entregable 6.5.2, Jan. 2010.
- AT4 wireless, Inabensa, **Universidad de Cantabria**, Universidad Politécnica de Cartagena, Universidad de Vigo, and Centro Tecnológico de Telecomunicaciones de Cataluña, “Nuevos Modelos, Técnicas y Mecanismos de gestión de las comunicaciones”, Proyecto CENIT mIO!, Entregable 6.5.3, Jan. 2010.
- AT4 Wireless, Robotiker, Telefónica I+D, Telvent, **Universidad de Cantabria**, Universidad de Castilla la Mancha, Universidad de Málaga, Universidad Rey Juan Carlos, and Worldnet21, “Análisis de sistemas de sensorización activos y balizamiento de pequeño tamaño y muy bajo consumo para un despliegue masivo de infraestructura de entornos inteligentes. Sensores y elementos inteligentes interconectados”, Proyecto CENIT mIO!, Entregable 5.3.4, Nov. 2010.
- AT4 Wireless, Universidad de Málaga, and **Universidad de Cantabria**, “Tendencias Tecnológicas en los Terminales Móviles”, Proyecto CENIT mIO!, Entregable 6.4.1, Jun. 2010.
- Inabensa, AT4 Wireless, Universidad de Málaga, Universidad de Vigo, and **Universidad de Cantabria**, “Investigación en comunicaciones integradas en los dispositivos de acceso. Requisitos de los dispositivos de acceso para la integración. Análisis de requisitos de la comunicación entre dispositivos de acceso y terminales móviles”, Proyecto CENIT mIO!, Entregable 6.1.2, Feb. 2010.
- Inabensa, AT4 Wireless, Worldnet21, Universidad de Vigo, Universidad de Málaga, **Universidad de Cantabria**, and Universidad Rey Juan Carlos, “Mejora en las tecnologías de comunicación entre el usuario y el entorno inteligente mediante técnicas de colaboración entre capas (cross-layer)”, Proyecto CENIT mIO!, Entregable 6.2.5, Feb. 2010.
- Telefónica I+D, **Universidad de Cantabria**, Telvent, Robotiker-Tecnalia, Caja Navarra, and CEMITEC, “Estudio de Disponibilidad de Tecnologías de Movilidad”, Proyecto CENIT mIO!, Entregable 4.1.2, Feb. 2010.
- AT4 Wireless, Inabensa, Robotiker-Tecnalia, Telefónica I+D, Telvent, **Universidad de Cantabria**, Universidad de Málaga, Universidad de Vigo, Universidad Rey Juan Carlos, and WorldNet21, “Análisis de interacción usuario-entorno en diferentes ambientes físicos”, Proyecto CENIT mIO!, Entregable 5.3.1, Nov. 2009.
- AT4 wireless, Inabensa, **Universidad de Cantabria**, Universidad de Vigo, and Centro Tecnológico de Telecomunicaciones de Cataluña, “Tendencias en gestión de comunicaciones”, Proyecto CENIT mIO!, Entregable 6.5.1, Mar. 2009.
- AT4 Wireless, **Universidad de Cantabria**, Universidad de Málaga, Universidad Rey Juan Carlos, WorldNet21, Inabensa, CTTC, TB Solutions, and Robotiker, “Investigación y evaluación de las tecnologías MAN y sus capacidades para proveer servicios ubicuos y en movilidad”, Proyecto CENIT mIO!, Entregable 6.3.1, Mar. 2009.

- Inabensa, AT4 Wireless, Worldnet21, Universidad de Vigo, **Universidad de Cantabria**, Universidad de Málaga, and Universidad Rey Juan Carlos, “Análisis de requisitos de conexión entre el usuario y el entorno inteligente proporcionando servicios personalizados en movilidad”, Proyecto CENIT mIO!, Entregable 6.2.4, Sep. 2009.
- Inabensa, AT4 Wireless, Worldnet21, Universidad Politécnica de Cartagena, Universidad de Málaga, **Universidad de Cantabria**, and Universidad Rey Juan Carlos, “Investigación en esquemas de acceso al medio de las tecnologías de comunicación entre el usuario y el entorno inteligente, para mejorar la eficiencia energética”, Proyecto CENIT mIO!, Entregable 6.2.2, Sep. 2009.
- Inabensa, AT4 Wireless, Worldnet21, Universidad de Vigo, Universidad de Málaga, **Universidad de Cantabria**, and Universidad Rey Juan Carlos, “Investigación en la selección óptima de la tecnología de comunicación entre el usuario y el entorno inteligente en función del consumo energético y del ancho de banda requerido”, Proyecto CENIT mIO!, Entregable 6.2.3, Sep. 2009.
- Inabensa, Universidad de Vigo, AT4 Wireless, **Universidad de Cantabria**, Universidad de Málaga, Universidad Rey Juan Carlos, and WorldNet21, “Investigación en tecnologías y elementos de interconexión entre el usuario y el entorno inteligente”, Proyecto CENIT mIO!, Entregable 6.2.1, Mar. 2009.
- Inabensa, Universidad Politécnica de Cartagena, AT4 Wireless, **Universidad de Cantabria**, and Universidad de Málaga, “Investigación en comunicaciones inalámbricas de corto alcance. Estado del arte. Caracterización y evaluación de estas tecnologías en el contexto del proyecto”, Proyecto CENIT mIO!, Entregable 6.1.1, Mar. 2009.
- Telefónica I+D, Telvent, Robotiker, **Universidad de Cantabria**, Caja Navarra, CEMITEC, WorldNet21, and Treelogic, “Especificación de requisitos de un entorno de creación de servicios inteligentes”, Proyecto CENIT mIO!, Entregable 4.6.1, Nov. 2009.
- Telefónica I+D, Telvent, Robotiker, **Universidad de Cantabria**, Caja Navarra, and CEMITEC, “Estado del Arte de Tecnologías de Prestación de Servicios en Movilidad”, Proyecto CENIT mIO!, Entregable 4.1.1, Mar. 2009.
- Telefónica I+D, Telvent, Robotiker, **Universidad de Cantabria**, Caja Navarra, and CEMITEC, “Estudio de las Tendencias en Tecnologías de Servicios de Distribución Comercial”, Proyecto CENIT mIO!, Entregable 4.5.1, Mar. 2009.
- Telefónica I+D and **Universidad de Cantabria**, “Sistema de autenticación y pagos basado en NFC en modo P2P”, Proyecto CENIT mIO!, Entregable - Activo Experimental 4.5.3_AE_3, Jun. 2009.
- Telvent, AT4 Wireless, Inabensa, Robotiker, Telefónica I+D, **Universidad de Cantabria**, Universidad de Málaga, Universidad de Vigo, Universidad Rey Juan Carlos, and WorldNet21, “Análisis de escenarios de implementación en entornos cerrados”, Proyecto CENIT mIO!, Entregable 5.1.2, Mar. 2009.

- Telvent, AT4 wireless, Robotiker, Telefónica I+D, **Universidad de Cantabria**, Universidad de Málaga, Universidad Rey Juan Carlos, and WorldNet21, “Análisis de escenarios de implementación en entornos abiertos (ciudad)”, Proyecto CENIT mIO!, Entregable 5.1.1, Mar. 2009.
- M. G. Genet, D. Zeglache, M. Ghader, D. Kraft, M. Bauer, E. Kovacs, J. Hoebeke, R. L. Olsen, M. Jacobsson, H. Thuvesson, J. Zeiss, S. Bessler, L. Sanchez, and **J. Lanza**, “Specifications of interfaces and interworking between PN networking architecture and service architectures”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 2.2.1, Feb. 2008.
- M. Jacobsson, I. Niemegeers, Y. Gu, T. Ahola, K. Ahola, M. Alutoin, M. Bauer, M. Girod-Genet, M. Ghader, A. Gouya, J. Hoebeke, G. Holderbeke, J. Jaen-Pallares, U. Javaid, P. Karlsson, **J. Lanza**, W. Louati, W. Louati, D.-E. Meddour, I. Moerman, R. L. Olsen, V. Prasad, L. Sanchez, J. Stoter, H. Thuvesson, and D. Zeglache, “PN secure networking frameworks, solutions and performance”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 2.3.2, Jun. 2008.
- L. Biard, D. Noguét, N. Sortur, A. Saxena, M. Shunmugam, L. Sanchez, **J. Lanza**, M. Saavela, and K. Ahola, “Complete MAGNET system platform towards Pilot Services”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 6.4.1, Oct. 2007.
- J. Hoebeke, I. Moerman, R. De Spiegelaere, S. Charfi, W. Louati, M. Girod-Genet, L. Sanchez, **J. Lanza**, J. Rico, T. Ahola, K. Ahola, M. Alutoin, and J. Jaen-Pallares, “Performance and Functionality Analysis of the PN Platform”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 6.3.2, Dec. 2007.
- J. Jaen Pallares, H. Affi, M. Argyropoulos, M. Bauer, S. Bessler, M. Girod-Genet, D. Kyriazanos, W. Louati, S. Mirzadeh, N. Prasad, J. Stoter, J. Zeiss, **J. Lanza**, and L. Sanchez, “Selections and Implementation of protocols and solutions in the view of PN-Platform”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 4.1.2, Feb. 2007.
- L. Sanchez, **J. Lanza**, K. Ahola, M. Alutoin, R. De Spiegelaere, J. Jaen-Pallares, S. Charfi, and M. Girod-Genet, “PN related platform towards Pilot Services”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 6.3.1, Dec. 2007.
- J. Zidbeck, T. Ahola, K. Ahola, M. Alutoin, M. Girod-Genet, J. Hoebeke, G. Holderbeke, J. Jaen-Pallares, **J. Lanza**, S. Charfi, I. Moerman, R. L. Olsen, L. Sanchez, D. Zeglache, and J. Zeiss, “MAGNET system secure networking components implementation”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 6.2.1, May 2007.
- J. Zidbeck, T. Ahola, K. Ahola, M. Alutoin, M. Girod-Genet, J. Hoebeke, G. Holderbeke, J. Jaen-Pallares, **J. Lanza**, S. Charfi, I. Moerman, R. L. Olsen, L. Sanchez, D. Zeglache, and J. Zeiss, “PN networking and security components conformance report”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 6.1.1, Jun. 2007.

- M. Bauer, **J. Lanza**, L. Sanchez, *et al.*, “Final interface specification for context aware components”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Internal Report 2.1.1, Sep. 2006.
- Y. Durand, D. Lattard, D. Mottier, T. Van Leeuwen, **J. Lanza**, A. Acha, L. Sanchez, and E. Gomez, “Platform performance and architecture requirements”, WISQUAS (Wireless Systems providing high QUALity Services), Deliverable 4.1, Apr. 2006.
- E. Gomez, L. Sanchez, **J. Lanza**, L. Arnaiz, L. Muñoz, C. Desset, S. Simoens, S. Gunaratne, D. Ktenas, and S. Mayrargue, “Efficient system simulation and behavioural modelling at all layers, with cross-layer metric modelling”, WISQUAS (Wireless Systems providing high QUALity Services), Deliverable 1.2, Oct. 2006.
- M. Jacobsson, M. Alutoin, M. Bauer, M. G. Genet, M. Ghader, A. Gouya, J. Hoebeke, G. Holderbeke, J. Jaen-Pallares, U. Javaid, P. Karlsson, **J. Lanza**, W. Louati, W. Louati, D.-E. Meddour, I. Moerman, R. L. Olsen, V. Prasad, L. Sanchez, J. Stoter, H. Thuvesson, and D. Zeghlache, “Specification of PN networking and security components”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 2.3.1, Dec. 2006.
- E. Kovacs, **J. Lanza**, L. Sanchez, K. Ahola, M. Jacobsson, M. Alutoin, and M. B. et al., “MAGNET System Specification”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Deliverable 1.1.1, Oct. 2006.
- L. Peters, T. Van Leeuwen, I. Moerman, A. Acha, L. Sanchez, **J. Lanza**, E. Gomez, and Y. Presumey, “Handover solutions for intra and inter system service continuity”, WISQUAS (Wireless Systems providing high QUALity Services), Deliverable 3.2, Mar. 2006.
- L. Sanchez, **J. Lanza**, *et al.*, “Preliminary interface specification for context aware and L2/L3 interfaces”, MAGNET Beyond (My personal Adaptive Global NET and Beyond), Milestone 2.1.1, Apr. 2006.
- P. Balamuralidhar, N. Marthur, M. De Sanctis, L. Sanchez, **J. Lanza**, J. Perez, G. P. Perrucci, K. Schoo, J. Rodriguez, M. Presser, D. Dahlhaus, and C. Peel, “MAC/RRM Schemes for WPAN (Update D3.3.2a)”, MAGNET (My personal Adaptive Global NET), Deliverable 3.3.2a, Dec. 2005.
- S. Lehtonen, M. Alutoin, K. Ahola, L. Sanchez, **J. Lanza**, L. Muñoz, W. Louati, W. Louati, M. Girod Genet, D. Zeghlache, G. Holderbeke, J. Hoebeke, J. Oksa, and A. Pietiläinen, “Early Prototype Demonstration based on Active Engine and PAN/PN based to PDAs/Laptops”, MAGNET (My personal Adaptive Global NET), Deliverable 2.5.3, Oct. 2005.
- R. L. Olsen, M. Ghader, M. Girod Genet, W. Louati, D. Zeghlache, H. P. Schwefel, L. Gavrilovska, M. Duspiva, M. Wellens, M. Petrova, L. Sanchez, and **J. Lanza**, “Service, Resource and Context Discovery system specification”, MAGNET (My personal Adaptive Global NET), Deliverable 2.2.3, Dec. 2005.

- L. Sanchez, **J. Lanza**, L. Muñoz, J. Hoebeke, G. Holderbeke, I. Moerman, W. Louati, W. Louati, M. Girod Genet, D. Zeghlache, K. Ahola, M. Alutoin, and S. Lehtonen, “Definition of full PAN/PN Network Terminal Prototyping System”, MAGNET (My personal Adaptive Global NET), Deliverable 2.5.2, Dec. 2005.
- M. De Sanctis, P. Giorgi, M. Presser, I. Ghauri, C. Peel, J. Perez, **J. Lanza**, L. Sanchez, P. Luis Muñoz Balamuralidhar, H. Choi, and F. Fitzek, “MAC/RRM Schemes for WPAN”, MAGNET (My personal Adaptive Global NET), Deliverable 3.3.2a, Oct. 2004.
- M. Ghader, R. L. Olsen, L. Sanchez, **J. Lanza**, L. Muñoz, J. Hoebeke, I. Moerman, M. Petrova, M. Wellens, M. Girod Genet, W. Louati, K. Masmoudi, D. Zeghlache, N. Köstering, S. Lehtonen, and R. Tafazolli, “Resource and Service Discovery: PN Solutions”, MAGNET (My personal Adaptive Global NET), Deliverable 2.2.1, Dec. 2004.
- M. Petrova, M. Jacobson, S. Oosthoek, J. Hoebeke, I. Moerman, H. Affi, D. Zeghlache, L. Muñoz, L. Sanchez, **J. Lanza**, M. Latvala, K. Nyberg, D. Sisalem, M. Presser, M. Ghader, and S. Mirzadeh, “Conceptual Secure PN Architecture”, MAGNET (My personal Adaptive Global NET), Deliverable 2.1.1, Dec. 2004.
- L. Sanchez, V. Gutierrez, O. Blanco, R. Agüero, R. San Juan, J. Choque, **J. Lanza**, J. A. Irastorza, L. Muñoz, Y. Liu, L. Gavrilovska, H. P. Schwefel, E. Puig, A. Markopoulos, J. Spanoudakis, S. Schallenburg, and S. Velentzas, “Link layer techniques in an ad-hoc WPAN environment”, PACWOMAN (Power Aware Communications for Wireless OptiMised personal Area Networks), Deliverable 5.3, Sep. 2004.
- L. Sanchez, **J. Lanza**, L. Muñoz, D. Zeghlache, W. Louati, W. Louati, I. Moerman, S. Pönkänen, S. Lehtonen, N. Köstering, S. Heemstra de Groot, and M. Jacobson, “Prototype concepts of a PAN/PN terminal and infrastructure network support”, MAGNET (My personal Adaptive Global NET), Deliverable 2.5.1, Dec. 2004.